STATE OF SOUTH DAKOTA
OFFICE OF PROCUREMENT MANAGEMENT
523 EAST CAPITOL AVENUE
PIERRE, SOUTH DAKOTA 57501-3182

Department of Social Services Office of Licensing and Accreditation - Management Information System

PROPOSALS ARE DUE NO LATER THAN MONDAY JULY 28, 2022

RFP 2814

BUYER:
Department of Social Services
Office of Licensing and Accreditation (OLA)

POC: Dawson Lewis
Dawson.Lewis@state.sd.us

READ CAREFULLY

FIRM NAME: _____ AUTHORIZED SIGNATURE: _____
(Digital Signature allowed)

ADDRESS: _____ TYPE OR PRINT NAME: _____

CITY/STATE: _____ TELEPHONE NO: _____

ZIP (9 DIGIT): _____ FAX NO: _____

FEDERAL TAX ID#: _____ E-MAIL: _____

PRIMARY CONTACT INFORMATION

CONTACT NAME: _____ TELEPHONE NO: _____

FAX NO: _____ E-MAIL: _____

1.0 GENERAL INFORMATION

1.1 PURPOSE OF REQUEST FOR PROPOSAL (RFP)

The State of South Dakota Department of Social Services (DSS) is issuing this RFP to solicit proposals from information technology (IT) vendors to implement a **management information system** (**MIS**) to support the operations of the Office of Licensing and Accreditation (OLA). The OLA was established to consolidate, standardize, and improve provider licensing and accreditation functions and information systems across various DSS programs. The current information systems utilized by OLA staff are comprised of multiple applications running within mainframe and client-server-based platforms, multiple spreadsheets and databases, and unstructured documents. Some of these systems are maintained and supported by the State's Bureau of Information and Telecommunications (BIT); others are maintained within OLA. Moreover, OLA staff need to access and/or exchange information with systems used by other programs within the department, including but not limited to the Family and Child Information System (FACIS) utilized by the department's Child Protective Services (CPS) division and the information systems used by DSS Child Care Services personnel.

For purposes of this RFP, the functions of OLA are defined, described and categorized as follows:

Initial provider licensing/accreditation and program registration/enrollment includes application intake and processing, any required background screening/checking, and ultimate determination of eligibility for licensing/accreditation
Provider life cycle management includes post-initial licensing/accreditation and program registration/enrollment tasks, including scheduled/planned reviews and recertifications
Provider monitoring and inspection (post initial licensing/accreditation and registration/enrollment) to ensure compliance with the conditions upon which licensing/accreditation was granted
Provider supports includes handling of provider inquiries, ongoing as-requested/as-needed provision of information, education, and training
Constituent supports includes handling of inquiries, complaints, and incident reports from the general public, some of whom may be receiving services from providers that OLA licenses/accredits
Provider quality and performance information management includes the collection of data that can be used to gage/rate provider quality and performance
Analytics and reporting that enables OLA to meet State and federal compliance requirements and supports performance evaluation, planning, and budgeting functions

The MIS being procured through this RFP will support licensure and accreditation processes for the following provider types:

- **Child Care Providers**: OLA licenses just under 800 child care providers across the state. There are five types of regulated (registered and licensed) providers: Registered family day care, licensed group family day care, licensed day care centers, licensed before and after school care, and informal child care providers.
- **Foster Care Families**: OLA licenses approximately 850 foster families across the state. The State has a goal of licensing 300 new families annually to increase the number of foster families. OLA also works very closely with the Division of Child Protection Services to place children with licensed foster families.
- **Child Welfare Agencies**: OLA licenses child placement agencies, group and residential treatment facilities, and independent living preparation programs. There are just under 40 licensed providers that support children in State custody.
- **Substance Use Disorder (SUD) and Community Mental Health Agencies**: OLA accredits approximately 56 agencies that offer SUD services or are a Community Mental Health facility.

OLA also manages the background screenings of providers and employees of said providers for child care, foster care resources, and child welfare agencies. Background screenings include screenings for child abuse and neglect through FACIS, State and national sex offender registry screenings, FBI and state criminal history using fingerprints, and out-of-state background screenings if the provider/employee

previously lived in another state. The MIS must facilitate the management of these background screening activities.

1.2 ISSUING OFFICE AND RFP REFERENCE NUMBER

The Office of Licensing & Accreditation is the issuing office for this document and all subsequent addenda relating to it, on behalf of the State of South Dakota, Department of Social Services. The reference number for the transaction is RFP #2814. Refer to this number on all proposals, correspondence, and documentation relating to the RFP.

Please refer to the Department of Social Services website link http://dss.sd.gov/keyresources/rfp.aspx for the RFP, any related questions/answers, changes to schedule of activities, amendments, etc.

1.3 LETTER OF INTENT

All interested offerors must submit a **Letter of Intent** to respond to this RFP.

The letter of intent must be received **by email** by the Department of Social Services no later than **Thursday June 30, 2022 and** must be addressed to Dawson.Lewis@state.sd.us. Place the following, exactly as written, in the subject line of your email: **Letter of Intent for RFP #2814.**

1.4 SCHEDULE OF ACTIVITIES (SUBJECT TO CHANGE)

RFP Publication	June 15, 2022
Letter of Intent to Respond Due	June 30, 2022
Deadline for Submission of Written Inquiries	July 7, 2022
Responses to Offeror Questions	July 21, 2022
Proposal Submission	Aug. 10, 2022, by 5:00 p.m. Central Time
Oral Presentations/discussions (if required)	August 29-Sept.1, 2022
Anticipated Award Decision/Start of Contract Negotiation	September 30, 2022

1.5 SUBMITTING YOUR PROPOSAL

An original proposal, one (1) identical copy, and one (1) digital copy loaded on a USB flash drive must be submitted.

A complete proposal must be comprised of **state-mandated forms and documents**; a **technical proposal** with responses as instructed to requirements outlined in this RFP, completion of applicable **attachments and** provision of **files** as instructed; and a **cost proposal file** completed as instructed. The original proposal document set must be signed in ink by an officer of the offeror legally authorized to bind the offeror to the proposal, and sealed in the form intended by the respondent. Proposals that are not complete as described above, or not properly signed, may be rejected.

No proposal may be accepted from, or any contract or purchase order awarded to any person, firm or corporation that is in arrears upon any obligations to the State of South Dakota, or that otherwise may be deemed irresponsible or unreliable by the State of South Dakota.

Proposals will be submitted in a sealed envelope that must be marked with the appropriate RFP Number and Title. The words “Sealed Proposal Enclosed” must be prominently denoted on the outside of the shipping container. **Proposals must be addressed and labeled as follows:**

Request For Proposal 2814 - Proposal Due 08/10/2022 5:00pm CDT
South Dakota Department of Social Services
Attention: Dawson Lewis, Operations Office
700 Governors Drive
Pierre SD 57501-2291

No punctuation is used in the address. The above address as displayed should be the only information in the address field.

1.6 CERTIFICATION REGARDING DEBARMENT, SUSPENSION, INELIGIBILITY AND VOLUNTARY EXCLUSION – LOWER TIER COVERED TRANSACTIONS

By signing and submitting this proposal, the offeror certifies that neither it nor its principals is presently debarred, suspended, proposed for debarment, declared ineligible, or voluntarily excluded from participation, by any Federal department or agency, from transactions involving the use of Federal funds. Where the offeror is unable to certify to any of the statements in this certification, the bidder shall attach an explanation to their offer.

1.7 NON-DISCRIMINATION STATEMENT

The State of South Dakota requires that all contractors, vendors, and suppliers doing business with any State agency, department, or institution, provide a statement of non-discrimination. By signing and submitting their proposal, the offeror certifies they do not discriminate in their employment practices with regard to race, color, creed, religion, age, sex, ancestry, national origin or disability.

1.8 RESTRICTION OF BOYCOTT OF ISRAEL

For contractors, vendors, suppliers, or subcontractors with five (5) or more employees who enter into a contract with the State of South Dakota that involves the expenditure of one hundred thousand dollars ($100,000) or more, by submitting a response to this solicitation or agreeing to contract with the State, the bidder or offeror certifies and agrees that the following information is correct:

The bidder or offeror, in preparing its response or offer or in considering proposals submitted from qualified, potential vendors, suppliers, and subcontractors, or in the solicitation, selection, or commercial treatment of any vendor, supplier, or subcontractor, has not refused to transact business activities, has not terminated business activities, and has not taken other similar actions intended to limit its commercial relations, related to the subject matter of the bid or offer, with a person or entity on the basis of Israeli national origin, or residence or incorporation in Israel or its territories, with the specific intent to accomplish a boycott or divestment of Israel in a discriminatory manner. It is understood and agreed that, if this certification is false, such false certification will constitute grounds for the State to reject the bid or response submitted by the bidder or offeror on this project and terminate any contract awarded based on the bid or response. The successful bidder or offeror further agrees to provide immediate written notice to the contracting executive branch agency if during the term of the contract it no longer complies with this certification and agrees such noncompliance may be grounds for contract termination.

1.9 MODIFICATION OR WITHDRAWAL OF PROPOSALS

Proposals may be modified or withdrawn by the offeror prior to the established due date and time.

No oral, telephonic, telegraphic or facsimile responses or modifications to informal, formal bids, or Request for Proposals will be considered unless previously approved.

1.10 OFFEROR INQUIRIES

Offerors may email inquiries concerning this RFP to obtain clarification of requirements. No inquiries will be accepted after the date in the Schedule of Activities. Email inquiries must be sent to Dawson.Lewis@state.sd.us with the following wording, exactly as written, in the subject line: **RFP 2814 Questions**.

The Department of Social Services (DSS) will respond to offerors' inquiries by posting offeror aggregated questions and Department responses on the DSS website at http://dss.sd.gov/keyresources/rfp.aspx no later than the date in the Schedule of Activities. For expediency, DSS may combine similar questions. Offerors may not rely on any other statements, either of a written or oral nature, that alter any specification or other term or condition of this RFP. Offerors will be notified in the same manner as indicated above regarding any modifications to this RFP.

1.11 PROPRIETARY INFORMATION

The proposal of the successful offeror(s) becomes public information.

Proprietary information can be protected under limited circumstances such as client lists and non-public financial statements. Pricing and service elements are not considered proprietary. An entire proposal may not be marked as proprietary. ***Offerors must clearly identify in their proposal's Executive Summary and mark in the body of the proposal any specific proprietary information they are requesting to be protected***. The Executive Summary must contain specific justification explaining why the information is to be protected. Proposals may be reviewed and evaluated by any person at the discretion of the State. All materials submitted become the property of the State of South Dakota and may be returned only at the State's option.

If an Offeror intends to submit a redacted copy of their proposal, it must submit the redacted copy along with the two required unredacted copies.

1.12 LENGTH OF CONTRACT

DSS intends to award a three (3) year contract with up to two (2) one-year extensions.

1.13 GOVERNING LAW

The venue for any and all legal action regarding or arising out of the transaction covered herein shall be solely in Hughes County, State of South Dakota. The laws of South Dakota shall govern this transaction.

1.14 DISCUSSIONS WITH OFFERORS (ORAL PRESENTATION/NEGOTIATIONS)

An oral presentation by an offeror to clarify a proposal may be required at the sole discretion of the State. However, the State may award a contract based on the initial proposals received without discussion with the offeror. If oral presentations are required, they will be scheduled after the submission of proposals. Oral presentations will be made at the offeror's expense.

This process is a Request for Proposal/Competitive Negotiation process. Each Proposal shall be evaluated, and each respondent shall be available for negotiation meetings at the State's request. The State reserves the right to negotiate on any and/or all components of every proposal submitted. From the time the proposals are submitted until the formal award of a contract, each proposal is considered a working document and as such, will be kept confidential. The negotiation discussions will also be held as confidential until such time as the award is completed.

2.0 STANDARD AGREEMENT TERMS AND CONDITIONS

Any contract or agreement resulting from this RFP will include, at minimum, the State's standard terms and conditions as seen in Attachment A. As part of the negotiation process, the contract terms listed in Attachment A may be altered or deleted.

Included in Attachment A are standard clauses pertaining to information system contracts from BIT. Because we expect a wide range of proposed solutions, we have included the widest number of possible clauses. We fully expect that, depending on the nature of your solution, clauses will be modified or removed in the final contract.

Offerors should indicate in their responses whether they have issues with specific contract terms. If the offeror does not indicate any contract term issues, then the State will assume the terms are acceptable.

3.0 SCOPE OF WORK

3.1 OVERVIEW

OLA is seeking an innovative, flexible, highly configurable, interoperable management information system (MIS) that is vendor-maintained, operated, and supported. The MIS must accommodate changing policies and business rules, interface with other information systems, leverage modern technologies, enable the adoption of operations and customer service best practices, and provide a first-class end user experience.

The State requires an MIS that supports the following OLA business functions:

3.1.1 Initial provider licensing/accreditation and program registration/enrollment. This includes provider application intake and processing, any required background checking, final determination on the application, and any related communication with the applying provider.

3.1.2 Provider life cycle management. This includes post-initial licensing/accreditation/registration/enrollment management activities including scheduled/planned reviews and recertifications.

3.1.3 Provider monitoring and inspection (post initial licensing/accreditation and registration/enrollment). This includes ad-hoc activities that ensure compliance with the conditions upon which licensing/accreditation was granted.

3.1.4 Provider supports. This includes handling of provider inquiries, ongoing provision of information, education, and training. These supports include the ability to provide information to providers via a web-accessible provider portal.

3.1.5 Constituent supports. This includes handling of constituent inquiries, complaints, and reported incidents tied to providers licensed/accredited by OLA. These supports include provision of information via a web-accessible public interface.

3.1.6 Provider quality and performance information management. This includes collection of data that can be used to assess/rate provider quality and performance, and generate associated dashboards, and reports.

3.1.7 Analytics and reporting. This includes activities that enable OLA to meet compliance requirements (State and federal) and support performance evaluation, planning, and budgeting functions.

Initially the MIS will support OLA functions specific to the following provider types:

Provider Type	General Description
1. Child Care Providers	Individuals and other entities that recipients of child care program subsidies can utilize under the terms of the Child Care Services program managed by DSS.
2. Foster Care Resources	Individuals and other entities that can serve as foster parents under terms prescribed by the Child Protective Services division of DSS.
3. Child Placement Agencies	Entities authorized to place children in State custody with foster care resources under terms prescribed by the Child Protective Services division of DSS.
4. Prevention, Substance Use Disorder (SUD) and Mental Health agencies	Entities authorized to provide certain services under terms prescribed by the Behavioral Health division of DSS - for more information refer to: *Community Behavioral Health (sd.gov)*.
5. Group and Residential Treatment Facilities	Facilities that must either be licensed as a residential treatment center under the provision of ARSD Ch. 67:42:08 or as an intensive residential treatment center under the provisions of ARSD Ch. 67:42:15

Since OLA's scope may change to encompass other provider types, the MIS must be architected such that additional provider types can be incorporated into the system without causing significant disruption and at minimal (if any) incremental cost.

It is the State's preference to procure an MIS that has already been implemented in another jurisdiction. South Dakota expects offerors to propose systems that have been architected to support OLA business functions as described previously and can be configured, without custom development/programming, to support OLA workflows and rules. In their responses to this RFP, offerors must demonstrate how they will provide an MIS that minimizes the amount of design and development work required to implement it. The State will not entertain proposals for *de novo* information system design and development.

The State will consider two MIS deployment scenarios:

- On-premises deployment - this type of deployment could entail a deployment of the MIS on servers located in BIT's data center or in South Dakota's government cloud computing environment administered by BIT.
- Hosted solution: the MIS would be hosted by the Offeror or a company under contract to the Offeror for hosting services.

3.2 TARGET ARCHITECTURE

The target architecture is an articulation of the desired information system's functionality and design that is aligned with both the IT industry and, where applicable, the broader DSS IT roadmap. The target architecture incorporates the following drivers and principles:

3.2.1. The system must be both highly configurable and interoperable. For example, system functionality that initially can only be accessed by "portals" connected to this system can be accessed eventually via broader DSS or even State government "portals".

3.2.2. The system must ensure that programs and services do not come across as fragmented and difficult to navigate from the perspective of providers. The system must streamline experiences for and interactions with providers and include self-service capabilities, electronic signature functionality, and the means to both submit information and complete transactions electronically.

3.2.3. The system must provide greater ability to leverage information – data and documents – on the part of both providers and agency personnel. This implies avoiding inefficiency and information integrity problems that result from, for instance, continuously requesting and maintaining multiple instances of essentially the same information. This also implies, ideally, having a single repository of provider information – both data and documents – irrespective of the programs in which a provider may participate.

3.2.4. The system must balance collaboration imperatives and the benefits of sharing system functionality and information with the unique needs of the programs and provider types being administered. The system cannot limit the ability of various programs to have their own workflows and rules within the system.

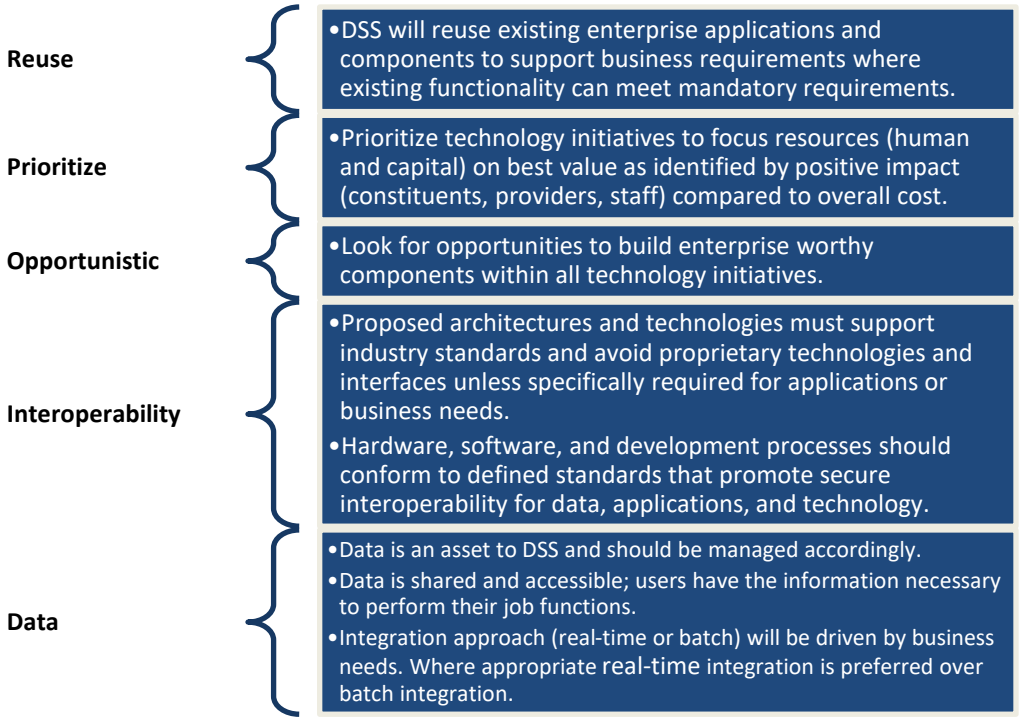
3.2.5. The system must have the ability to grow and change without being encumbered by technology constraints. This necessitates exceptional system configurability, but it also has implications on internal capacity for system administration – ideally the system would be "friendly" enough for many systems administration tasks to be managed by a properly trained OLA resource.

3.2.6. The system must allow for easy access via a mobile device. This includes the potential for the system to be accessible as an "app" on such a device. This capability will be of particular value for the management of foster care providers.

3.2.7. The system must provide analytics and reporting functionality that supports OLA personnel performance management, licensed/accredited **provider** performance management, verification of compliance with State and federal laws and regulations, budgeting and personnel planning, and program design and optimization. This functionality includes the ability to selectively "push" information to the public at large, recipients, and governance bodies.

Moreover, the desired system must conform with certain business architecture principles being applied across DSS as DSS undertakes the modernization of its information systems. These principles are outlined in Figure 1.

Figure 1: DSS Business Architecture Principles



3.3 REQUIREMENTS

3.3.1 While MIS requirements are detailed elsewhere in the RFP (refer to Section 3.3.3), critical MIS functionality can be grouped into four major categories or "modules":

1. **A web-accessible provider portal** with single sign-on and multiple functions available therein, including:
   - The ability for providers/organzations to record and store certain information (data and documents), submit applications, and upload supporting documentation.
   - The ability for providers to submit background check requests, review the status of their applications, and obtain a real-time update on said status, among other features.
   - A public facing website that enables providers to access authoritative information about programs, applications, etc.

2. **A web-accessible public interface** with the following functions:
   - The ability for members of the general public to submit concerns/complaints to the State.
   - Searchable licensed/accredited provider database by provider name, type, location, etc.
   - The ability for search for inspections, corrective action plans and other actions/events linked to licensed/accredited providers.

3. **An operations management module** with a rich set of functions designed to empower OLA personnel and facilitate their work, including:
   - The ability to configure and administer rules, workflows, and transaction management processes based on OLA policies and procedures.
   - The ability to monitor and intervene, as needed, to ensure timely, efficient processing of different types of transactions.
   - The ability to process provider applications with minimal human touch.
   - Enables Outlook calendaring/scheduling of the wide variety of activities conducted by OLA staff.
   - The ability to complete and document provider inspections/reviews/investigations.
   - The ability to generate and issue certificates.
   - The ability to generate provider and constituent communications with minimal human intervention by leveraging rules, workflows and templates.

- The ability to track progress in identifying available foster care resources and the placement of foster children.
- The ability to capture and retain certain indexed documents, linked as appropriate to a particular provider, constituent, and/or OLA staff member.
- The ability to interact with providers and constituents, including the ability to receive and manage inquiries and other transactions electronically, the ability to code these interactions and - based on roles, rules, and workflows - "refer" or “route” the interactions to appropriate parties.

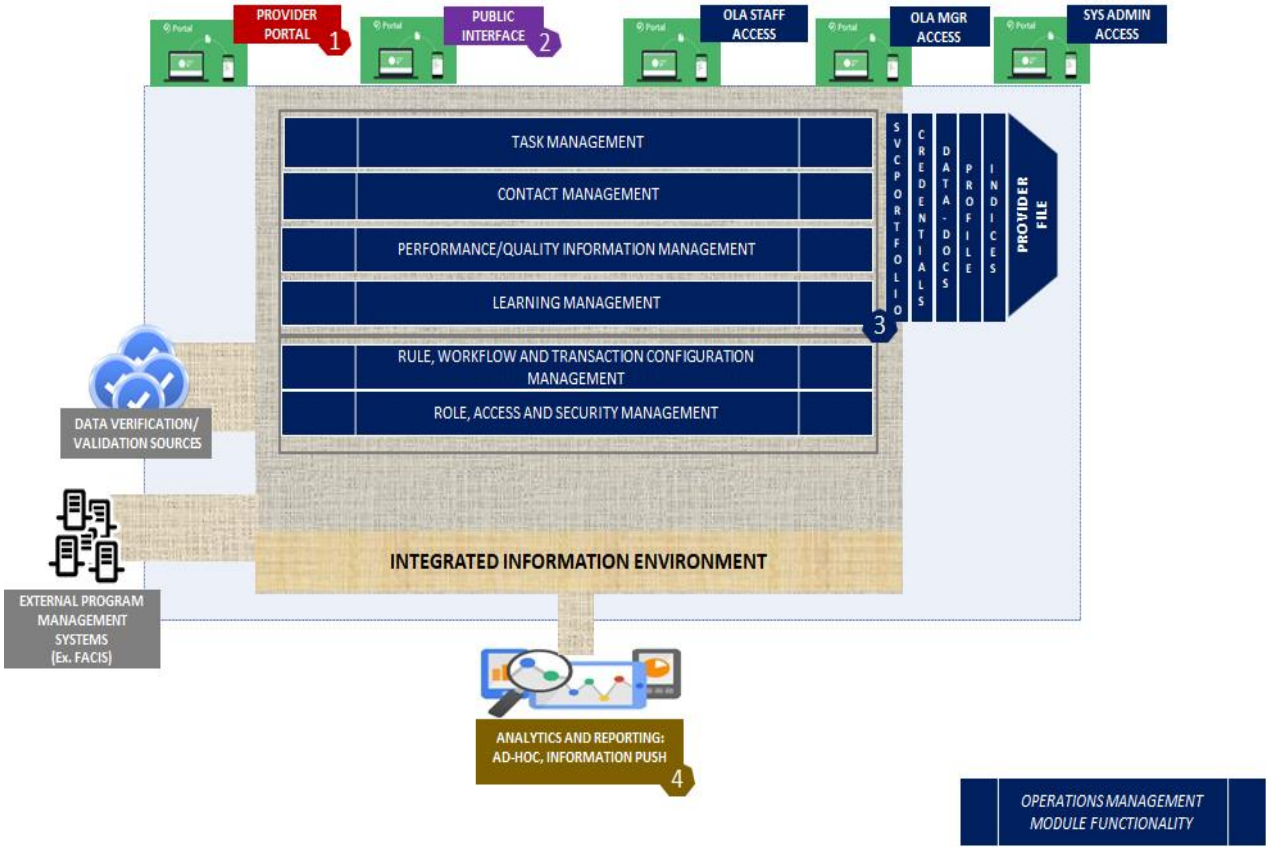
4. **An analytics and reporting module** that enables OLA to meet compliance requirements (State and federal) and conduct performance evaluation, planning, and budgeting functions. This module must:
   - Support data collection, querying and analytics, reporting and dashboarding, and benchmarking/trending/tracking.
   - Facilitate generation of ad-hoc reports and changes to reports built into the module prior to go-live without requiring Contractor involvement.

3.3.2 Ideally these features would work off an **integrated information environment. I**nformation related to activities across all OLA functions would all be housed in a single information store, which would make it easier for data to be retrieved and maintained, improve data quality and integrity, and facilitate its reuse (for instance, a provider would not have to submit the same data multiple times in response to inquiries). Additionally, several MIS capabilities will require interfaces to other information systems, particularly FACIS and the systems used by the Child Care Services program (refer to Section 3.3.3); at present these systems are operated, maintained and supported by BIT. Finally, to facilitate the transition to the MIS certain data and documents will be targeted for migration and as-needed conversion into the system’s integrated information environment. Five sets of data and documents are targeted for migration and as-needed conversion (more information on these data/documents and the associated information systems is provided in the RFP Attachment D:

- Child care provider data, from one of the systems used to manage the state’s child care services program.
- Child care provider inspection records, from one of the systems used to manage the state’s child care services program.
- Licensing documentation, including certificates issued, for child welfare agencies; currently these documents are housed in PDF format in a database that supports a constituent-facing website.
- Licensing documentation, including certificates issued, for SUD and community mental health agencies; currently these documents are housed in PDF format.
- Select data and documents about providers that are expected to be active at the time of the migration/conversion. Currently these data reside mainly in Microsoft Excel files, whereas the documents are either Microsoft Word files or PDF-formatted files stored in shared drives or in a department-specific instance of the state’s File Director document management system.

Figure 2 illustrates the Department’s vision for the OLA Management Information System.

Figure 2: Office of Licensing and Accreditation Future Management Information System – Concept Diagram (information system "modules" are numbered)



3.3.3 Matrices that detail MIS requirements can be found in Attachments B through E. In addition to responding to specific questions in this RFP, Offerors must include completed requirement matrices in their proposals. The purpose of the completed requirement matrices is to ascertain an Offeror's ability to meet functional, technical, interface, and reporting requirements and discuss their approach to meeting them.

1. A matrix of Functional Requirements can be found in **Attachment B** – **Functional Requirements**
2. A matrix of Technical Requirements can be found in **Attachment C** – **Technical Requirements**
3. A matrix of Interface Requirements can be found in **Attachment D** – **Interface Requirements**
4. A matrix of Required Reports can be found in **Attachment E** – **Report Requirements**

3.3.4 Additionally, **Attachment F** details requirements that govern **information system management**; Offerors must describe how they will meet all of these requirements in their responses to this RFP. Information system management requirements include:

- Approach to implementation including the project management methodology which the Offeror would employ – implementation includes all of the activities leading to the system's go-live,
- Approach to maintenance, operations, support and, if applicable, hosting,
- Approach to information system and information security management – including but not limited to management of system access rights,
- Approach to managing information system performance and related metrics, and
- Approach to turnover in the event the contract for system maintenance, operations, support (and, if applicable, hosting) is terminated.

3.3.5 Finally, the MIS and its supplier must meet requirements for all South Dakota government agency information systems established by BIT. These requirements include the following:

1. Any contract or agreement resulting from this RFP will include the State's standard IT contract terms listed in **Exhibit A**, along with any additional contract terms as negotiated by the parties. As part of the negotiation process the contract terms listed in **Exhibit A** may be altered or deleted. The offeror should indicate in its response any issues it has with specific contract terms. If the offeror does not indicate that there are any issues with any contract terms, then the State will assume those terms are acceptable to the offeror.

2. All suppliers of information systems to South Dakota government agencies must respond to the BIT Security and Vendor Questionnaire; refer to **Attachment H**. Offerors shall complete Attachment H and include the completed attachment in its response to this RFP.

3. The Offeror must include a diagram giving an overview of its proposed system in its response to this RFP. The diagram must provide an understanding of the system's architecture, the various functional components or modules of the system, and how it would exchange information with other systems. Additionally, if applicable the diagram should provide an understanding of how the system would be hosted. This diagram shall be provided in the proposal as a separate document (i.e. an attachment to the offeror's response to RFP questions). The file must be named "(Your Name) Hosted System Diagram" or "(Your Name) On-Premise System Diagram" depending on the offeror's proposed approach to system deployment. If the Offeror is proposing both an on-premises deployment and a hosted solution, the Offeror will provide two diagrams labeled as instructed.

4. Offerors must state whether its proposed system will operate in a virtualized environment and, in that scenario, identify and describe all differences, restrictions or limitations of its proposed system with respect to operation, licensing, support, certification, warranties, and any other details that may impact its proposed system when hosted in a virtualized environment. Offerors will provide this information in the same file in which they provide the system overview diagram described in (3), above.

5. Offerors will be required to maintain test environments for their proposed systems. The test environments will be used for pre go-live testing, and may also be accessed and employed at the discretion of BIT. The test environments will be maintained by the offeror. A test environment that mirrors the production system's code base must be made available for user acceptance testing. All resource and licensing costs associated with keeping test environments available must be borne by the offeror. At BIT's discretion, any code changes made by the offeror, either during this project or thereafter, will be placed in test environments first. It is at BIT's discretion if the code changes are applied by BIT or the offeror. If the code testing delays a project's timeline, a change management process should be followed, and the State will not be charged for this project change.

6. All information systems acquired by the State that are hosted by the offeror, including Software as a Service, or hosted by a third-party for the offeror will be subjected to security scans by BIT prior to and after go-live; alternatively the offeror will provide detailed security scan reports as requested by BIT in a format prior approved by BIT. A detailed security report must consist of at least:
   - The system that was evaluated (URL if possible, but mask it if needed).
   - The categories that were evaluated (example: SQL injection, cross site scripting, etc.)
   - What were the general findings, (meaning how many SQL injection issues were found, what was the count per category).
   - Technical detail of each issue found. (where was it found – web address, what was found, the http response if possible).

   If the Offeror is proposing a hosted solution, it must provide a security scan report in its response to this RFP; the scan report sent in with the proposal can be redacted by the offeror.

   Offerors must build the cost of any security scans done by the offeror or the offeror's costs associated with the State's scans into their cost proposals.

7. Any website or web application hosted by the offeror that generates email cannot use "@state.sd.us" as the originating domain name per state security policy.

8. As part of the State's Identity and Access Management (IAM) strategy, the proposed system will need to integrate with the State of South Dakota's standard identity management service single sign on (SSO) which enables custom control of how citizens and/or state employees sign up, sign in, and manage their profiles. The SSO supports two industry standard protocols: OpenID Connect and OAuth 2.0 (preferred). This identity management will handle password recovery.

9. Multi-factor Authentication (MFA) is required for all application Administrators.

10. Hosting and Data Access Requirements - The contract doubles as an agreement for the State to own the data tables and is able to manipulate data, run reports as needed, pull code tables, access raw data and develop dashboards as needed through Microsoft Power BI, ESRI, Tableau and associated platforms.

11. The offeror must describe how the proposed system can adapt to necessary interfaces using widely adopted open application programming interfaces (APIs) and standards. Additionally, DSS expects that the offeror will make available/expose software services and publish documentation for those software services that would enable third party developers to interface other business applications. A detailed description of these capabilities shall be included in the proposal.

12. Background checks - the offeror must include the following statement in its proposal:

    (Company name here) acknowledges and affirms that it understands that the (company name here) employees who have access to production Personally Identifiable Information (PII), data protected under the Family Educational Rights and Privacy Act (FERPA), Protected Health Information (PHI), Federal Tax Information (FTI), any information defined under state statute as confidential or have access to secure facilities will have fingerprint based background checks. These background checks will be used to check the criminal history records of the State as well as the Federal Bureau of Investigation's records. (Company name here) acknowledges and affirms that this requirement will extend to include any Subcontractor's, Agents, Assigns and or Affiliated Entities employees.

13. Non-standard hardware and software: State standard hardware and software should be utilized unless there is a reason not to. If your proposal will use non-standard hardware or software, you must first obtain State approval. If your proposal recommends using non-standard hardware or software, the proposal should very clearly indicate what non-standard hardware or software is being proposed and why it is necessary to use non-standard hardware or software to complete the project requirements. The costs of such non-standard hardware or software should be reflected in your cost proposal. The work plan should also account for the time needed to complete the Moratorium Process. See http://bit.sd.gov/standards/, for lists of the State's standards. The proposal should also include a link to your hardware and software specifications. If non-standard hardware or software is used, the project plan and the costs must include service desk and field support, since BIT can only guarantee best effort support for standard hardware and software. If any software development may be required in the future, hourly development rates must be stated. The project plan must include the development and implementation of a disaster recovery plan since non-standard hardware and software will not be covered by the State's disaster recovery plan. This must also be reflected in the costs.

4.0 PROPOSAL REQUIREMENTS AND COMPANY QUALIFICATIONS

4.1 The offeror is cautioned that it is the offeror's sole responsibility to submit information related to the evaluation categories and that the State of South Dakota is under no obligation to solicit such information if it is not included with the proposal. The offeror's failure to submit such information may cause an adverse impact on the evaluation of the proposal.

4.2 **Offeror's Contacts**: Offerors and their agents (including subcontractors, employees, consultants, or anyone else acting on their behalf) must direct all of their questions or comments regarding the RFP, the evaluation, etc. to the point of contact of the buyer of record indicated on the first page of this RFP. Offerors and their agents may not contact any state employee other than the buyer of record regarding any of these matters during the solicitation and evaluation process. Inappropriate contacts are grounds for suspension and/or exclusion from specific procurements. Offerors and their agents who have questions regarding this matter should contact the buyer of record.

4.3 An offeror may be required to submit a copy of its most recent independently audited financial statement.

4.4 References: Offerors must provide the following information related to at ***least*** two previous or current contracts performed by the offeror's organization which are similar to the requirements of this RFP:

a. Name, address, and telephone number of client/contracting agency and a representative of that agency who may be contacted for verification of all information submitted;
b. Dates of the contract;
c. A brief, written description of the specific services performed and requirements thereof;
d. For previous contracts, an explanation of why the contracts are no longer in effect; and
e. A brief explanation of how that contract is relevant to this RFP.

4.5 An offeror must submit information that demonstrates its availability and familiarity with the locale in which the project (s) are to be implemented. Specifically, an offeror shall describe its knowledge of/experience with South Dakota state government agencies and health and human services providers, as well as elaborate on any challenges or issues specific to South Dakota and how it intends to address them.

4.6 An offeror must detail examples that document its ability and proven history to handle special project constraints; at a minimum, address time, personnel availability constraints as well as the ability to work virtually/remotely in your response to this requirement.

4.7 If an offeror's proposal is not accepted by the State, the proposal will not be reviewed/evaluated. Proposals will not be accepted for the following reasons:

- Not received on time
- Incorrectly addressed or labeled
- Not signed by Offeror as required

5.0 PROPOSAL RESPONSE FORMAT

5.1 An original hard copy, one hard copy, and an electronic copy (all pertinent files stored in an USB flash drive) of the proposal must be submitted. All proposal documents must be page numbers. Additionally, offerors will provide a table of contents that references the applicable documents and page numbers.

5.2 The technical proposal must be organized, page-constrained and tabbed as follows:

RFP Section/ Attachment #	Description	Page Limit (if Applicable)
	Completed and Signed Request for Proposal Form	N/A
N/A	Table of Contents	N/A

1.11	Executive Summary – Narrative and, if applicable, accompanying figures, charts and tables that describe: - The offeror's understanding of the information system functionality requested through this RFP and the rationale/drivers behind this RFP, - The major features of the offeror's proposed information system, - The offeror's approach to implement and operate, maintain, support (and, if applicable, host) the system, and - The offeror's experience and capabilities which, in the offeror's estimation, position to offeror to meet RFP requirements. The summary must also indicate any proposal information the offeror wants to protect (refer to Section 1.11) and any requirements that cannot be met by the offeror. The reader should be able to determine the essence of the proposal by reading the executive summary. Proprietary information requests should be identified in this section.	7
3.2, 3.3.1, 3.3.2	Point-by-Point Response to Target Architecture and Requirements outlined in Sections 3.2, 3.3.1 and 3.3.2	25 (including all narrative and diagrams, excluding required reports)
3.3.3/B	Completed Functional Requirements Matrix	N/A
3.3.3/C	Completed Technical Requirements Matrix	N/A
3.3.3/D	Completed Interface Requirements Matrix	N/A
3.3.3/E	Completed Report Requirements Matrix	N/A
3.3.4/F	Point-by-Point Response to Information System Requirements outlined in Attachment F	25 (including all narrative and diagrams, excluding sample documents)
3.3.5/G	Response to Standard IT Contract Terms	N/A
3.3.5/H	Completed BIT Security and Vendor Questionnaire	N/A
3.3.5	Information System Diagram(s) and, If Applicable, Information on Virtualized Environment - separate file(s)	N/A
3.3.5	Point-by-Point Response to Information System Requirements outlined in Section 3.3.5 other than the response to Standard IT Contract Terms, completed attachments and required files	10
4.4	References (Minimum 2)	3
4.5	Information Regarding Availability and Familiarity with the Locale	2
4.6	Examples and Experience Regarding Special Project Constraints	3
N/A	Model Project Plan: A two-level breakdown of implementation activities with expected phase and activity duration that incorporates major project milestones, major project deliverables and expected dependencies across activities. The Model Project Plan shall be built in Microsoft Project or other project management application. For the electronic copy of the proposal, offerors must include a PDF-formatted version of the Model Project Plan and a version of the Model Project Plan in its native file format. For purposes of creating the Model Project Plan, the Offeror shall assume a twelve-month	N/A

	implementation. The Offeror must detail any assumptions used to create the Model Project Plan. Additionally, the Offeror shall provide suggestions on conditions that would enable MIS implementation in a shorter time period.	

5.3 Cost Proposal. Cost will be evaluated independently from the technical proposal. Offerors may submit a cost proposal for a hosted solution and/or an on-premises solution; refer as needed to definitions of "hosted" and "on-premises" solutions in Section 3.1 of this RFP. All costs related to the provision of the required services must be included in each cost proposal offered. The cost proposal must be submitted in a separate sealed envelope labeled "Cost Proposal". See sections 1.5 and 7.0 for more information related to the cost proposal.

6.0 PROPOSAL EVALUATION AND AWARD PROCESS

6.1 After determining that a proposal satisfies the mandatory requirements stated in the Request for Proposal, the evaluator(s) shall use subjective judgment in conducting a comparative assessment of the proposal by considering each of the following criteria listed in order of importance:

6.1.1 Specialized expertise, capabilities, and technical competence as demonstrated by the proposed approach and methodology to meet the project requirements.

6.1.2 Record of past performance, including price and cost data from previous projects, quality of work, ability to meet schedules, cost control, and contract administration;

6.1.3 Cost proposal;

6.1.4 Proposed project management methodology and toolset.

6.1.5 Resources available to perform the work, including any specialized services, within the specified time limits for the project;

6.1.6 Availability to the project locale;

6.1.7 Ability and proven history in handling special project constraints, and

6.1.8 Familiarity with South Dakota, its culture, population needs, and the project locale.

6.2 Experience and reliability of the offeror's organization are considered subjectively in the evaluation process. Therefore, the offeror is advised to submit any information which documents successful and reliable experience in past performances, especially those performances related to the requirements of this RFP.

6.3 The qualifications of the personnel proposed by the offeror to perform the requirements of this RFP, whether from the offeror's organization or from a proposed subcontractor, will be subjectively evaluated. Therefore, the offeror should submit detailed information related to the experience and qualifications, including education and training, of proposed personnel.

6.4 The State reserves the right to reject any or all proposals, waive technicalities, and make award(s) as deemed to be in the best interest of the State of South Dakota.

6.5 **Award:** The requesting agency and the highest ranked offeror shall mutually discuss and refine the scope of services for the project and shall negotiate terms, including compensation and performance schedule.

6.5.1 If the agency and the highest ranked offeror are unable for any reason to negotiate a contract at a compensation level that is reasonable and fair to the agency, the agency shall, either orally or in writing, terminate negotiations with the contractor. The agency may then negotiate with the next highest ranked contractor.

6.5.2 The negotiation process may continue through successive offerors, according to agency ranking, until an agreement is reached or the agency terminates the contracting process.

6.5.3 Only the response of the vendor awarded work becomes public. Responses to work orders for vendors not selected and the evaluation criteria and scoring for all proposals are not public. Vendors may submit a redacted copy with the full proposal as stated in Section 1.12 Proprietary Information. SDCL 1-27-1.5 and See SDCL 1-27-1.5 and 1-27-1.6.

7.0 **COST PROPOSAL**

Offerors must complete the supplied cost proposal file in its native Microsoft Excel file format as instructed; refer to the README worksheet in that file for detailed instructions. Offerors must submit the completed cost proposal file as instructed in Sections 1.5 and 5.3 of this RFP.

ATTACHMENT A – Sample Contract

STATE OF SOUTH DAKOTA
DEPARTMENT OF SOCIAL SERVICES
OFFICE OF LICENSING AND ACCREDITATION

Consultant Contract
For Consultant Services
Between

State of South Dakota
Department of Social Services
Office of Licensing and Accreditation
700 Governors Drive
Pierre, SD 57501-2291

Referred to as Consultant

Referred to as State

The State hereby enters into a contract (the "Agreement" hereinafter) for consultant services with the Consultant. While performing services hereunder, Consultant is an independent contractor and not an officer, agent, or employee of the State of South Dakota.

1. CONSULTANT'S South Dakota Vendor Number is .

2. PERIOD OF PERFORMANCE:
   This Agreement shall be effective as of and shall end on, unless sooner terminated pursuant to the terms hereof.

   Agreement is the result of request for proposal process, RFP #_____

3. PROVISIONS:
   A. The Purpose of this Consultant contract:
      1.

      2. Does this Agreement involve Protected Health Information (PHI)? YES ( ) NO (X)
         If PHI is involved, a Business Associate Agreement must be attached and is fully incorporated herein as part of the Agreement (refer to attachment) .

      3. The Consultant will use state equipment, supplies or facilities.

   B. The Consultant agrees to perform the following services (add an attachment if needed.):
      1.

   C. The State agrees to:
      1.

      2. Make payment for services upon satisfactory completion of services and receipt of bill. Payment will be in accordance with SDCL 5-26.

      3. Will the State pay Consultant expenses as a separate item?
         YES ( ) NO (X)
         If YES, expenses submitted will be reimbursed as identified in this Agreement.

   D. The TOTAL CONTRACT AMOUNT will not exceed $.

4. BILLING:
   Consultant agrees to submit a bill for services within (30) days following the month in which services were provided. Consultant will prepare and submit a monthly bill for services. Consultant agrees to submit a final bill within 30 days of the Agreement end date to receive payment for completed services. If a final bill cannot be submitted in 30 days, then a written request for extension of time and explanation must be provided to the State.

5. TECHNICAL ASSISTANCE:
   The State agrees to provide technical assistance regarding Department of Social Services rules, regulations and policies to the Consultant and to assist in the correction of problem areas identified by the State's monitoring activities.

6. LICENSING AND STANDARD COMPLIANCE:
   The Consultant agrees to comply in full with all licensing and other standards required by Federal, State, County, City or Tribal statute, regulation, or ordinance in which the service and/or care is provided for the duration of this Agreement. The Consultant will maintain effective internal controls in managing the federal award. Liability resulting from noncompliance with licensing and other standards required by Federal, State, County, City or Tribal statute, regulation or ordinance or through the Consultant's failure to ensure the safety of all individuals served is assumed entirely by the Consultant.

7. ASSURANCE REQUIREMENTS:
   The Consultant agrees to abide by all applicable provisions of the following: Byrd Anti Lobbying Amendment (31 USC 1352), Executive orders 12549 and 12689 (Debarment and Suspension), Drug-Free Workplace, Executive Order 11246 Equal Employment Opportunity, Title VI of the Civil Rights Act of 1964, Title VIII of the Civil Rights Act of 1968, Section 504 of the Rehabilitation Act of 1973, Title IX of the Education Amendments of 1972, Drug Abuse Office and Treatment Act of 1972, Comprehensive Alcohol Abuse and Alcoholism Prevention, Treatment and Rehabilitation Act of 1970, Age Discrimination Act of 1975, Americans with Disabilities Act of 1990, Pro-Children Act of 1994, Hatch Act, Health Insurance Portability and Accountability Act (HIPAA) of 1996 as amended, Clean Air Act, Federal Water Pollution Control Act, Charitable Choice Provisions and Regulations, Equal Treatment for Faith-Based Religions at Title 28 Code of Federal Regulations Part 38, the Violence Against Women Reauthorization Act of 2013 and American Recovery and Reinvestment Act of 2009, as applicable; and any other nondiscrimination provision in the specific statute(s) under which application for Federal assistance is being made; and the requirements of any other nondiscrimination statute(s) which may apply to the award.

8. COMPLIANCE WITH EXECUTIVE ORDER 2020-01:
   By entering into this Agreement, Consultant certifies and agrees that it has not refused to transact business activities, it has not terminated business activities, and it has not taken other similar actions intended to limit its commercial relations, related to the subject matter of this Agreement, with a person or entity that is either the State of Israel, or a company doing business in or with Israel or authorized by, licensed by, or organized under the laws of the State of Israel to do business, or doing business in the State of Israel, with the specific intent to accomplish a boycott of divestment of Israel in a discriminatory manner. It is understood and agreed that, if this certification is false, such false certification will constitute grounds for the State to terminate this Agreement. Consultant further agrees to provide immediate written notice to the State if during the term of this Agreement it no longer complies with this certification and agrees such noncompliance may be grounds for termination of this Agreement.

9. RETENTION AND INSPECTION OF RECORDS:

The Consultant agrees to maintain or supervise the maintenance of records necessary for the proper and efficient operation of the program, including records and documents regarding applications, determination of eligibility (when applicable), the provision of services, administrative costs, statistical, fiscal, other records, and information necessary for reporting and accountability required by the State. The Consultant shall retain such records for a period of six years from the date of submission of the final expenditure report. If such records are under pending audit, the Consultant agrees to hold such records for a longer period upon notification from the State. The State, through any authorized representative, will have access to and the right to examine and copy all records, books, papers or documents related to services rendered under this Agreement. State Proprietary Information retained in Consultant's secondary and backup systems will remain fully subject to the obligations of confidentiality stated herein until such information is erased or destroyed in accordance with Consultant's established record retention policies.

All payments to the Consultant by the State are subject to site review and audit as prescribed and carried out by the State. Any over payment of this Agreement shall be returned to the State within thirty days after written notification to the Consultant.

10. WORK PRODUCT:
Consultant hereby acknowledges and agrees that all reports, plans, specifications, technical data, drawings, software system programs and documentation, procedures, files, operating instructions and procedures, source code(s) and documentation, including those necessary to upgrade and maintain the software program, State Proprietary Information, as defined in the Confidentiality of Information paragraph herein, state data, end user data, Protected Health Information as defined in 45 CFR 160.103, and all information contained therein provided to the State by the Consultant in connection with its performance of service under this Agreement shall belong to and is the property of the State and will not be used in any way by the Consultant without the written consent of the State.

Paper, reports, forms, software programs, source code(s) and other materials which are a part of the work under this Agreement will not be copyrighted without written approval of the State. In the unlikely event that any copyright does not fully belong to the State, the State nonetheless reserves a royalty-free, non-exclusive, and irrevocable license to reproduce, publish, and otherwise use, and to authorize others to use, any such work for government purposes.

Consultant agrees to return all information received from the State to State's custody upon the end of the term of this Agreement, unless otherwise agreed in a writing signed by both parties.

11. TERMINATION:
This Agreement may be terminated by either party hereto upon thirty (30) days written notice. In the event the Consultant breaches any of the terms or conditions hereof, this Agreement may be terminated by the State for cause at any time, with or without notice. Upon termination of this Agreement, all accounts and payments shall be processed according to financial arrangements set forth herein for services rendered to date of termination.

12. FUNDING:
This Agreement depends upon the continued availability of appropriated funds and expenditure authority from the Legislature for this purpose. If for any reason the Legislature fails to appropriate funds or grant expenditure authority, or funds become unavailable by operation of the law or federal funds reduction, this Agreement will be terminated by the State. Termination for any of these reasons is not a default by the State nor does it give rise to a claim against the State.

13. ASSIGNMENT AND AMENDMENTS:
This Agreement may not be assigned without the express prior written consent of the State. This Agreement may not be amended except in writing, which writing shall be expressly identified as a part hereof, and be signed by an authorized representative of each of the parties hereto.

14. CONTROLLING LAW:
This Agreement shall be governed by and construed in accordance with the laws of the State of South Dakota, without regard to any conflicts of law principles, decisional law, or statutory provision which would require or permit the application of another jurisdiction's substantive law. Venue for any lawsuit pertaining to or affecting this Agreement shall be resolved in the Circuit Court, Sixth Judicial Circuit, Hughes County, South Dakota.

15. SUPERCESSION:
All prior discussions, communications and representations concerning the subject matter of this Agreement are superseded by the terms of this Agreement, and except as specifically provided herein, this Agreement constitutes the entire agreement with respect to the subject matter hereof.

16. IT STANDARDS:
Any software or hardware provided under this Agreement will comply with state standards which can be found at http://bit.sd.gov/standards/.

17. SEVERABILITY:
In the event that any provision of this Agreement shall be held unenforceable or invalid by any court of competent jurisdiction, such holding shall not invalidate or render unenforceable any other provision of this Agreement, which shall remain in full force and effect.

18. NOTICE:
Any notice or other communication required under this Agreement shall be in writing and sent to the address set forth above. Notices shall be given by and to the Division being contracted with on behalf of the State, and by the Consultant, or such authorized designees as either party may from time to time designate in writing. Notices or communications to or between the parties shall be deemed to have been delivered when mailed by first class mail, provided that notice of default or termination shall be sent by registered or certified mail, or, if personally delivered, when received by such party.

19. SUBCONTRACTORS:
The Consultant may not use subcontractors to perform the services described herein without express prior written consent from the State. The State reserves the right to reject any person from the Agreement presenting insufficient skills or inappropriate behavior.

The Consultant will include provisions in its subcontracts requiring its subcontractors to comply with the applicable provisions of this Agreement, to indemnify the State, and to provide insurance coverage for the benefit of the State in a manner consistent with this Agreement. The Consultant will cause its subcontractors, agents, and employees to comply with applicable federal, state and local laws, regulations, ordinances, guidelines, permits and requirements and will adopt such review and inspection procedures as are necessary to assure such compliance. The State, at its option, may require the vetting of any subcontractors. The Consultant is required to assist in this process as needed.

20. STATE'S RIGHT TO REJECT:
The State reserves the right to reject any person or entity from performing the work or services contemplated by this Agreement, who present insufficient skills or inappropriate behavior.

21. HOLD HARMLESS:
The Consultant agrees to hold harmless and indemnify the State of South Dakota, its officers, agents and employees, from and against any and all actions, suits, damages, liability or other proceedings which may arise as the result of performing services hereunder. This section does not require the Consultant to be responsible for or defend against claims or damages arising solely from errors or omissions of the State, its officers, agents or employees.

22. INSURANCE:
Before beginning work under this Agreement, Consultant shall furnish the State with properly executed Certificates of Insurance which shall clearly evidence all insurance required in this Agreement. The Consultant, at all times during the term of this Agreement, shall obtain and maintain in force insurance coverage of the types and with the limits listed below. In the event a substantial change in insurance, issuance of a new policy, cancellation or nonrenewal of the policy, the Consultant agrees to provide immediate notice to the State and provide a new certificate of insurance showing continuous coverage in the amounts required. Consultant shall furnish copies of insurance policies if requested by the State.

A. Commercial General Liability Insurance:
Consultant shall maintain occurrence-based commercial general liability insurance or an equivalent form with a limit of not less than $1,000,000 for each occurrence. If such insurance contains a general aggregate limit, it shall apply separately to this Agreement or be no less than two times the occurrence limit.

B. Business Automobile Liability Insurance:
Consultant shall maintain business automobile liability insurance or an equivalent form with a limit of not less than $500,000 for each accident. Such insurance shall include coverage for owned, hired, and non-owned vehicles.

C. Worker's Compensation Insurance:
Consultant shall procure and maintain Workers' Compensation and employers' liability insurance as required by South Dakota law.

D. Professional Liability Insurance:
Consultant agrees to procure and maintain professional liability insurance with a limit not less than $1,000,000.

(Medical Health Professional shall maintain current general professional liability insurance with a limit of not less than one million dollars for each occurrence and three million dollars in the aggregate. Such insurance shall include South Dakota state employees as additional insureds in the event a claim, lawsuit, or other proceeding is filed against a state employee as a result of the services provided pursuant to this Agreement. If insurance provided by Medical Health

Professional is provided on a claim made basis, then Medical Health Professional shall provide "tail" coverage for a period of five years after the termination of coverage.)

23. CERTIFICATION REGARDING DEBARMENT, SUSPENSION, INELIGIBILITY, AND VOLUNTARY EXCLUSION:
Consultant certifies, by signing this Agreement, that neither it nor its principals are presently debarred, suspended, proposed for debarment, declared ineligible, or voluntarily excluded from participation in this transaction by the federal government or any state or local government department or agency. Consultant further agrees that it will immediately notify the State if during the term of this Agreement either it or its principals become subject to debarment, suspension or ineligibility from participating in transactions by the federal government, or by any state or local government department or agency.

24. CONFLICT OF INTEREST:
Consultant agrees to establish safeguards to prohibit employees or other persons from using their positions for a purpose that constitutes or presents the appearance of personal or organizational conflict of interest, or personal gain as contemplated by SDCL 5-18A-17 through 5-18A-17.6. Any potential conflict of interest must be disclosed in writing. In the event of a conflict of interest, the Consultant expressly agrees to be bound by the conflict resolution process set forth in SDCL 5-18A-17 through 5-18A-17.6.

25. SSAE
The selected offeror will be required to provide a copy of its most recent System and Organization Controls, Statement on Standards for Attestation Engagements (SOC 1 SSAE18) report, then annually thereafter for the term of the agreement. For SOC 1 SSAE 18 the offeror must identify which of the following can be provided on an annual basis: SOC 1, SOC 2, or SOC 3.

26. CONFIDENTIALITY OF INFORMATION:
For the purpose of the sub-paragraph, "State Proprietary Information" shall include all information disclosed to the Consultant by the State. Consultant acknowledges that it shall have a duty to not disclose any State Proprietary Information to any third person for any reason without the express written permission of a State officer or employee with authority to authorize the disclosure. Consultant shall not: (i) disclose any State Proprietary Information to any third person unless otherwise specifically allowed under this Agreement; (ii) make any use of State Proprietary Information except to exercise rights and perform obligations under this Agreement; (iii) make State Proprietary Information available to any of its employees, officers, agents or consultants except those who have agreed to obligations of confidentiality at least as strict as those set out in this Agreement and who have a need to know such information. Consultant is held to the same standard of care in guarding State Proprietary Information as it applies to its own confidential or proprietary information and materials of a similar nature, and no less than holding State Proprietary Information in the strictest confidence. Consultant shall protect confidentiality of the State's information from the time of receipt to the time that such information is either returned to the State or destroyed to the extent that it cannot be recalled or reproduced. State Proprietary Information shall not include information that (i) was in the public domain at the time it was disclosed to Consultant; (ii) was known to Consultant without restriction at the time of disclosure from the State; (iii) that is disclosed with the prior written approval of State's officers or employees having authority to disclose such information; (iv) was independently developed by Consultant without the benefit or influence of the State's information; (v) becomes known to Consultant without restriction from a source not connected to the State of South Dakota. State's Proprietary Information shall include names, social security numbers, employer numbers, addresses and all other data about applicants, employers or other clients to whom the State provides services of any kind. Consultant understands that this information is confidential and protected under applicable State law at SDCL 1-27-1.5, modified by SDCL 1-27-1.6, SDCL 28-1-29, SDCL 28-1-32, and SDCL 28-1-68 as applicable federal regulation and agrees to immediately notify the State if the information is disclosed, either intentionally or inadvertently. The parties mutually agree that neither of them shall disclose the contents of the Agreement except as required by applicable law or as necessary to carry out the terms of the Agreement or to enforce that party's rights under this Agreement. Consultant acknowledges that the State and its agencies are public entities and thus are bound by South Dakota open meetings and open records laws. It is therefore not a breach of this Agreement for the State to take any action that the State reasonably believes is necessary to comply with the South Dakota open records or open meetings laws. If work assignments performed in the course of this Agreement require additional security requirements or clearance, the Consultant will be required to undergo investigation.

27. REPORTING PROVISION:

Consultant agrees to report to the State any event encountered in the course of performance of this Agreement which results in injury to any person or property, or which may otherwise subject Consultant, or the State of South Dakota or its officers, agents or employees to liability. Consultant shall report any such event to the State immediately upon discovery.

Consultant's obligation under this section shall only be to report the occurrence of any event to the State and to make any other report provided for by their duties or applicable law. Consultant's obligation to report shall not require disclosure of any information subject to privilege or confidentiality under law (e.g., attorney-client communications). Reporting to the State under this section shall not excuse or satisfy any obligation of Consultant to report any event to law enforcement or other entities under the requirements of any applicable law.

28. DAVIS-BACON ACT
When required by Federal program legislation, all prime construction contracts in excess of $2,000 awarded by non-Federal entities must include a provision for compliance with the Davis-Bacon Act (40 U.S.C. 3141-3144, and 3146-3148) as supplemented by Department of Labor regulations (29 CFR Part 5, "Labor Standards Provisions Applicable to Contracts Covering Federally Financed and Assisted Construction").

29. COMPLIANCE WITH 40 U.S.C. 3702 AND 3704
Where applicable, all contracts awarded by the non-Federal entity in excess of $100,000 that involve the employment of mechanics or laborers must include a provision for compliance with 40 U.S.C. 3702 and 3704, as supplemented by Department of Labor regulations (29 CFR Part 5).

30. FUNDING AGREEMENT AND "RIGHTS TO INVENTION"
If the Federal award meets the definition of "funding agreement" under 37 CFR §401.2 (a) and the Consultant wishes to enter into a contract with a small business firm or nonprofit organization regarding the substitution of parties, assignment or performance of experimental, developmental, or research work under that "funding agreement," the Consultant must comply with the requirements of 37 CFR Part 401, "Rights to Inventions Made by Nonprofit Organizations and Small Business Firms Under Government Grants, Contracts and Cooperative Agreements," and any implementing regulations issued by the awarding agency.

AUTHORIZED SIGNATURES:

In witness hereto, the parties signify their agreement by affixing their signatures hereto.

Consultant Signature	Date
Consultant Printed Name	
State - DSS Division Director	Date
State - DSS Chief Financial Officer Jason Simmons	Date
State – DSS Cabinet Secretary Laurie R. Gill	Date
State – BIT Commissioner Jeffrey Clines	Date

State Agency Coding:

CFDA #				
Company				
Account				
Center Req				
Center User				
Dollar Total				

DSS Program Contact Person _____
Phone _____

DSS Fiscal Contact Person Contract Accountant
Phone 605 773-3586

Consultant Program Contact Person _____
Phone _____
Consultant Program Email Address _____

Consultant Fiscal Contact Person _____
Phone _____
Consultant Fiscal Email Address _____

SDCL 1-24A-1 states that a copy of all consulting contracts shall be filed by the State agency with the State Auditor within five days after such contract is entered into and finally approved by the contracting parties. For further information about consulting contracts, see the State Auditor's policy handbook.

Exhibit A – Bureau of Information and Telecommunications (BIT) Contract clauses.

BIT is charged by the state with making sure that all technology used is compatible with State Standards. Also, that the data of our citizens is safeguarded. Because we do not know what methods an offeror will use to access data we have included the widest possible number of clauses.

Depending on your proposed solution certain of these clauses may not be needed and will be removed from the final contract.

UNRESOLVED BREACH OF THE AGREEMENT

In the event of an unresolved breach of this agreement, the parties acknowledge that damages from the breach will be difficult or impossible to measure or quantify. The parties agree that in the event of a breach, the Consultant shall pay, as liquidated damages, and not as a penalty, the sum of $ 1,000,000 or the amount paid by the State to the Consultant plus 10 %, whichever is less which the parties agree is a fair and reasonable method of computing the damages caused by the breach.

CONFIDENTIALITY OF INFORMATION

For purposes of this paragraph, "State Proprietary Information" shall include all information disclosed to the Consultant by the State. The Consultant, and Consultant's Subcontractors, Agents, Assigns and/or Affiliated Entities shall not disclose any State Proprietary Information to any third person for any reason without the express written permission of a State officer or employee with authority to authorize the disclosure. The Consultant, and Consultant's Subcontractors, Agents, Assigns and/or Affiliated Entities shall not: (i) disclose any State Proprietary Information to any third person unless otherwise specifically allowed under this agreement; (ii) make any use of State Proprietary Information except to exercise rights and perform obligations under this agreement; (iii) make State Proprietary Information available to any of its employees, officers, agents or third party Consultants except those who have a need to access such information and who have agreed to obligations of confidentiality at least as strict as those set out in this agreement. The Consultant, and Consultant's Subcontractors, Agents, Assigns and/or Affiliated Entities is held to the same standard of care in guarding State Proprietary Information as it applies to its own confidential or proprietary information and materials of a similar nature, and no less than holding State Proprietary Information in the strictest confidence. The Consultant, and Consultant's Subcontractors, Agents, Assigns and/or Affiliated Entities shall protect the confidentiality of the State's information from the time of receipt to the time that such information is either returned to the State or destroyed to the extent that it cannot be recalled or reproduced. The Consultant, and Consultant's Subcontractors, Agents, Assigns and/or Affiliated Entities agree to return all information received from the State to State's custody upon the end of the term of this agreement, unless otherwise agreed in a writing signed by both parties. State Proprietary Information shall not include information that:

(i) was in the public domain at the time it was disclosed to the Consultant, and Consultant's Subcontractors, Agents, Assigns and/or Affiliated Entities;
(ii) was known to the Consultant, and Consultant's Subcontractors, Agents, Assigns and/or Affiliated Entities without restriction at the time of disclosure from the State;
(iii) that was disclosed with the prior written approval of State's officers or employees having authority to disclose such information;
(iv) was independently developed by the Consultant, and Consultant's Subcontractors, Agents, Assigns and/or Affiliated Entities without the benefit or influence of the State's information;
(v) becomes known to the Consultant, and Consultant's Subcontractors, Agents, Assigns and/or Affiliated Entities without restriction from a source not connected to the State of South Dakota.

State's Proprietary Information can include names, social security numbers, employer numbers, addresses and other data about applicants, employers or other clients to whom the State provides services of any kind. Consultant understands that this information is confidential and protected under State law. The parties mutually agree that neither of them nor any Consultant, and Consultant's Subcontractors, Agents, Assigns and/or Affiliated Entities shall disclose the contents of this agreement except as required by applicable law or as necessary to carry out the terms of the agreement or to enforce that party's rights under this agreement. Consultant acknowledges that the State and its agencies are public entities and thus may be bound by South Dakota open meetings and open records laws. It is therefore not a breach of this agreement for the State to take any action that the State reasonably believes is necessary to comply with South Dakota open records or open meetings laws.

CYBER LIABILITY INSURANCE

The Consultant shall maintain cyber liability insurance with liability limits in the amount of $ 5,000,000 to protect any and all State data the Consultant receives as part of the project covered by this agreement including State data that may reside on

devices, including laptops and smart phones, utilized by Consultant employees, whether the device is owned by the employee or the Consultant. If the Consultant has a contract with a third-party to host any State data the Consultant receives as part of the project under this agreement, then the Consultant shall include a requirement for cyber liability insurance as part of the contract between the Consultant and the third-party hosting the data in question. The third-party cyber liability insurance coverage will include State data that resides on devices, including laptops and smart phones, utilized by third-party employees, whether the device is owned by the employee or the third-part Consultant. The cyber liability insurance shall cover expenses related to the management of a data breach incident, the investigation, recovery and restoration of lost data, data subject notification, call management, credit checking for data subjects, legal costs, and regulatory fines. Before beginning work under this Agreement, the Consultant shall furnish the State with properly executed Certificates of Insurance which shall clearly evidence all insurance required in this Agreement and which provide that such insurance may not be canceled, except on 30 days prior written notice to the State. The Consultant shall furnish copies of insurance policies if requested by the State. The insurance will stay in effect for 2 years after the work covered by this agreement is completed.

CHANGE MANAGEMENT PROCESS

From time to time it may be necessary or desirable for either the State or the Consultant to propose changes to the Services provided. Such changes shall be effective only if they are in writing and contain the dated signatures of authorized representatives of both parties. Unless otherwise indicated, a change or amendment shall be effective on the date it is signed by both parties. Automatic upgrades to any software used by the Consultant to provide any services that simply improve the speed, efficiency, reliability, or availability of existing services and do not alter or add functionality, are not considered "changes to the Services" and such upgrades will be implemented by the Consultant on a schedule no less favorable than that provided by the Consultant to any other customer receiving comparable levels of services.

WORK PRODUCTS

The Consultant shall be responsible for the professional quality, technical accuracy, timely completion, and coordination of all services furnished by the Consultant and any subcontractors, if applicable, under this Agreement. It shall be the duty of the Consultant to assure that the services and the system are technically sound and in conformance with all pertinent Federal, State and local statutes, codes, ordinances, resolutions and other regulations. The Consultant shall, without additional compensation, correct or revise any errors or omissions in its work products.

Consultant hereby acknowledges and agrees that all reports, plans, specifications, technical data, miscellaneous drawings, agreements, State Proprietary Information, any information discovered by the State,
Personally Identifiable Information (PII), data protected under Family Educational Rights and Privacy Act (FERPA), Protected Health Information (PHI), Federal Tax Information (FTI) or any information defined under state statute as confidential, and all information contained therein provided to the State by the Consultant in connection with its performance under this Agreement shall belong to and is the property of the State and will not be used in any way by the Consultant without the written consent of the State.

Papers, reports, forms or other material which are a part of the work under this Agreement will not be copyrighted without written approval of the State. In the event that any copyright does not fully belong to the State, the State reserves a royalty-free, non-exclusive, non-transferable, and irrevocable license to reproduce, publish, and otherwise use and to authorize others to use on the State's behalf any such work for government purposes.

PRODUCT CONFORMITY

The State has twelve (12) months following final acceptance of the product(s) delivered by the Consultant pursuant to this Agreement to verify that the product(s) conform to the requirements of this Agreement and perform according to the Consultant's system design specifications. Upon the State's recognition of an error, deficiency, or defect, the Consultant shall be notified by the State. The notification shall cite any specific deficiency (deficiency being defined as the Consultant having performed incorrectly with the information previously provided by the State, not the Consultant having to modify a previous action due to additional and/or corrected information from the State). The Consultant, at no additional charge to the State, shall provide a correction or provide a mutually acceptable plan for correction within thirty-days following the receipt of the State's notice to the Consultant. If the Consultant's correction is inadequate to correct the deficiency, or defect, or if error recurs, the State may, at its option, act to correct the problem. The Consultant shall be required to reimburse the State for any such costs incurred or the State will consider this to be a breach of the agreement. Payment by the Consultant pursuant to this provision does not waive any other rights and remedies available to the State.

CURING OF BREACH OF AGREEMENT

In the event of a breach of these representations and warranties the State may, at the State's discretion, provide the Consultant with the opportunity to rectify the breach. The Consultant shall immediately, after notice from the State, begin work on curing such breaches. If the notice is telephonic the State will provide, at the Consultant's request, a written notice to reaffirm the telephonic notice. If such problem remains unresolved after three days, at State's discretion, Consultant will send, at Consultant's sole expense, at least one qualified and knowledgeable representative to the State's site where the system is located. This representative will continue to address and work to remedy the deficiency, failure, malfunction, defect, or problem at the site. The rights and remedies provided in this paragraph are in addition to any other rights or remedies provided in this Agreement or by law.

DOMAIN NAME OWNERSHIP

Any website(s) that the Consultant creates as part of this project must have the domain name registered by and owned by the State. If as part of this project the Consultant is providing a service that utilizes a website with the domain name owned by the Consultant, the Consultant must give thirty (30) days' notice before abandoning the site. If the Consultant intends to sell the site to another party the Consultant must give the State thirty days (30) notice and grant the State the right of first refusal. For any site or domain, whether hosted by the Consultant or within the State web infrastructure, any and all new web content should first be created in a development environment and then subjected to security scan before being approved for a move up to the production level.

SOFTWARE FUNCTIONALITY AND REPLACEMENT

The software licensed by the Consultant to the State provides the following functionality:

Initial provider licensing/accreditation and program registration/enrollment includes application intake and processing, any required background screening/checking, and ultimate determination of eligibility for licensing/accreditation
Provider life cycle management includes post-initial licensing/accreditation and program registration/enrollment tasks, including scheduled/planned reviews and recertifications
Provider monitoring and inspection (post initial licensing/accreditation and registration/enrollment) to ensure compliance with the conditions upon which licensing/accreditation was granted
Provider supports includes handling of provider inquiries, ongoing as-requested/as-needed provision of information, education, and training
Constituent supports includes handling of inquiries, complaints, and incident reports from the general public, some of whom may be receiving services from providers that OLA licenses/accredits
Provider quality and performance information management includes the collection of data that can be used to gage/rate provider quality and performance
Analytics and reporting that enables OLA to meet State and federal compliance requirements and supports performance evaluation, planning, and budgeting functions

The Consultant agrees that:

A. If in the opinion of the State the Consultant reduces or replaces the functionality contained in the licensed product and provides this functionality as a separate or renamed product, the State shall be entitled to license such software product at no additional license or maintenance fee.
B. If in the opinion of the State the Consultant releases an option, future product, purchasable product or other release that has substantially the same functionality as the software product licensed to the State, and it ceases to provide maintenance for the older software product, the State shall have the option to exchange licenses for such replacement product or function at no additional charge. This includes situations where the Consultant discontinues the licensed product and recommends movement to a new product as a replacement option regardless of any additional functionality the replacement product may have over the licensed product.

LICENSE GRANT

A. The Consultant grants to the State a perpetual, worldwide, nonexclusive license to use the software and associated documentation, plus any additional software which shall be added by mutual agreement of the parties during the term of this agreement.
B. The license usage model is based on ….. (Clearly describe license model, i.e. concurrent users, total employees, etc. to be completed at the time the contract is written)

C. The license grant may be extended to any contractors, subcontractors, outsourcing consultants and others who have a need to use the software for the benefit of the State.

SOURCE CODE ESCROW

A. Deposit in Escrow: "Source Code" means all source code of the Software, together with all commentary and other materials supporting, incorporated into or necessary for the use of such source code, including all supporting configuration, documentation, and other resource files and identification by Consultant and version number of any software (but not a license to such third-party software) used in connection with the source code and of any compiler, assembler, or utility used in generating object code.

1. Within ninety (90) days of the effective date, Consultant shall deposit the Source Code for the software with a nationally recognized software escrow company (subject to the approval of the State, not to be unreasonably withheld) (the "Escrow Agreement"). Within thirty (30) days after delivery to Customer of any major update, Consultant shall deposit the Source Code for such update with the Escrow Agent pursuant to the Escrow Agreement. For all other updates, Consultant shall deposit the Source Code for such updates on a semiannual basis with the Escrow Agent pursuant to the Escrow Agreement.

2. The parties agree that the Escrow Agreement is an "agreement supplementary to" the Agreement as provided in Section 365(d) of Title 11, United States Code (the "Bankruptcy Code"). Immediately upon termination of this Agreement, the Source Code shall be released back to Consultant.

B. Conditions for release: The State will have the right to obtain the Source Code in accordance with and subject to the terms and conditions of this Section and the Escrow Agreement provided that all of the following three conditions are met (collectively a "Release Event"):

1. Consultant winds down its business or liquidates its business under a Chapter 7 Bankruptcy proceeding; or Consultant discontinues maintenance and support to the Software,

2. No entity has succeeded to Consultant's obligations to provide maintenance and support on the Software in accordance with the Agreement in effect between the parties, and

3. The State is not in breach of its obligations under this Agreement.

C. Source Code: In no event shall the State have the right to use the Source Code "barring a release event" for any purpose, and the State is specifically prohibited from using the Source Code to reverse engineer, develop derivative works or to sublicense the right to use the Source Code to any other person or entity for any purpose. Customer will also be obligated to treat the Source Code as Confidential Information of Consultant under the Agreement.

The cost for establishing and maintaining the Escrow Account will be that of the State.

FEDERAL INTELLECTUAL PROPERTY BANKRUPTCY PROTECTION ACT

The Parties agree that the State shall be entitled to all rights and benefits of the Federal Intellectual Property Bankruptcy Protection Act, Public Law 100-506, codified at 11 U.S.C. 365(n), and any amendments thereto. The State also maintains its termination privileges if the Consultant enters bankruptcy.

SECURITY RISK RATING

The Consultant will provide the State with its security rating before work commences. A security rating is an objective indicator of the Consultant's security posture and practices done though an independent external assessment. The security rating is reported as a single number or grade. The rating company's detailed assessment must be provided. If the State finds the security rating to be inadequate the State and the Consultant will do a mutually agreed to remediation plan to bring the Consultant's rating to an acceptable level or at the State's discretion, terminate the Agreement with no further obligation. The consultant will have a security rating done annually by an industry recognized security rating company. The Consultant will provide their security rating to the State annually. If the State finds the security rating to be inadequate the State and the Consultant will do a mutually agreed to remediation plan to bring the Consultant's rating to an acceptable level or the State can terminate the Agreement with no further obligation.

DATA RECOVERY
The Consultant must be able to recover the State's data in the same state it was sent to the Consultant for testing and production. If the Consultant system or the third-party system that is hosting data for the Consultant is subjected to a disaster severe enough to implement disaster recovery procedures, then recovery of the State data will follow the disaster recovery requirements for Recovery Time Objective and Recovery Point Objective agreed to by the State and the Consultant.

REJECTION OR EJECTION OF CONSULTANT, AND CONSULTANT'S SUBCONTRACTORS, AGENTS, ASSIGNS AND/OR AFFILIATED ENTITIES EMPLOYEE(S)
The State, at its option, may require the vetting of any of the Consultant, and Consultant's Subcontractors, Agents, Assigns and/or Affiliated Entities. The Consultant is required to assist in this process as needed.

The State reserves the right to reject any person from participating in the project or require the Consultant to remove from the project any person the State believes is detrimental to the project or is considered by the State to be a security risk. The State will provide the Consultant with notice of its determination, and the reasons for the rejection or removal if requested by the Consultant. If the State signifies that a potential security violation exists with respect to the request, the Consultant shall immediately remove the individual from the project.

PROVISION OF DATA
Upon notice of termination by either party, the State will be provided by the Consultant all current State Data in a non-proprietary form. Upon the effective date of the termination of the agreement, the State will again be provided by the Consultant with all current State Data in a non-proprietary form. State Data is any data produced or provided by the State as well as any data produced or provided for the State by a third-party.

THREAT NOTIFICATION
Upon becoming aware of a credible security threat with the Consultant's product(s) and or service(s) being used by the State, the Consultant or any subcontractor supplying product(s) or service(s) to the Consultant needed to fulfill the terms of this Agreement will notify the State within two (2) business days of any such threat. If the State requests, the Consultant will provide the State with information on the threat. A credible security threat consists of the discovery of an exploit that a person considered an expert on Information Technology security believes could be used to breach one or more aspects of a system that is holding State data, or a product provided by the Consultant.

SECURITY INCIDENT NOTIFICATION
The Consultant will implement, maintain and update Security Incident procedures that comply with all State standards and Federal and State requirements. A Security Incident is a violation of any BIT security or privacy policies or contract agreements involving sensitive information, or the imminent threat of a violation. The BIT security policies can be found in the Information Technology Security Policies attached as Attachmen H. The State requires notification of a Security Incident involving any of the State's sensitive data in the Contractor's possession. State Data is any data produced or provided by the State as well as any data produced or provided for the State by a third-party. The parties agree that, to the extent probes and reconnaissance scans common to the industry constitute Security Incidents, this Agreement constitutes notice by Consultant of the ongoing existence and occurrence of such Security Incidents for which no additional notice to the State shall be required. Probes and scans include, without limitation, pings and other broadcast attacks in the Consultant's firewall, port scans, and unsuccessful log-on attempts, as long as such probes and reconnaissance scans do not result in a Security Incident as defined above. Except as required by other legal requirements the Consultant shall only provide notice of the incident to the State. The State will determine if notification to the public will be by the State or by the Consultant. The method and content of the notification of the affected parties will be coordinated with, and is subject to approval by the State, unless required otherwise by legal requirements. If the State decides that the Consultant will be distributing, broadcasting to or otherwise releasing information on the Security Incident to the news media, the State will decide to whom the information will be sent, and the State must approve the content of any information on the Security Incident before it may be distributed, broadcast or otherwise released. The Consultant must reimburse the State for any costs associated with the notification, distributing, broadcasting or otherwise releasing information on the Security Incident.

A. The Consultant shall notify the State Contact within twelve (12) hours of the Consultant becoming aware that a Security Incident has occurred.

If notification of a Security Incident to the State Contact is delayed because it may impede a criminal investigation or jeopardize homeland or federal security, notification must be given to the State within twelve (12) hours after law-enforcement provides permission for the release of information on the Security Incident.

B. Notification of a Security Incident at a minimum is to consist of the nature of the data exposed, the time the incident occurred and a general description of the circumstances of the incident. If not all of the information is available for the notification within the specified time period Consultant shall provide the State with all of the available information along with the reason for the incomplete notification. A delay in excess of twelve (12) hours is acceptable only if it is necessitated by other legal requirements.

C. At the State's discretion within 2 days the consultant must provide to the State all data available including: (i) Name of and contact information for the Consultant's Point of Contact for the Security Incident: (ii) date and time of the Security Incident; (iii) date and time the Security Incident was discovered: (iv) description of the Security Incident including the data involved, being as specific as possible; (v) the potential number of records, and if unknown the range of records; (vi) address where the Security Incident occurred: and, (vii) the nature of the technologies involved. Notifications must be sent electronically and encrypted via NIST or other applicable federally approved encryption techniques. If there are none use AES256 encryption. Consultant shall use the term "data incident report" in the subject line of the email. If not all of the information is available for the notification within the specified time period Consultant shall provide the State with all of the available information along with the reason for the incomplete information. A delay in excess of twelve (12) hours is acceptable only if it is necessitated by other legal requirements.

D. If the information from the Breach of System Security includes State of South Dakota residents whose personal or protected information was, or is reasonably believed to have been, acquired by an unauthorized person consultant must notify the resident(s) in accordance with South Dakota Codified Law (SDCL) Chapter 22-40. Requirements of this chapter include that if there are two-hundred and fifty (250) or more residents' records involved the State of South Dakota Attorney General (ATG) must be notified. Both notifications must be within sixty (60) days of the discovery of the breach. The Consultant shall also notify, without unreasonable delay, all consumer reporting agencies, as defined under 15 U.S.C. § 1681a in effect as of January 1, 2018, and any other credit bureau or agency that compiles and maintains files on consumers on a nationwide basis, of the timing, distribution, and content of the notice. The Consultant is not required to make a disclosure under this section if, following an appropriate investigation and notice to the ATG, the Consultant reasonably determines that the breach will not likely result in harm to the affected person. The Consultant shall document the determination under this section in writing and maintain the documentation for not less than three (3) years. These statements of requirements from SDCL 22-40 are neither comprehensive nor all inclusive, and consultant shall comply with all applicable provisions of that chapter.

The requirements of section D do not replace the requirements of sections A, B and C but are in addition to them.

HANDLING OF SECURITY INCIDENT

At the State's discretion the Consultant will preserve all evidence regarding a security incident including but not limited to communications, documents, and logs. The Consultant will also:

(i) fully investigate the incident,
(ii) cooperate fully with the State's investigation of, analysis of, and response to the incident,
(iii) make a best effort to implement necessary remedial measures as soon as it is possible and,
(iv) document responsive actions taken related to the Security Incident, including any post-incident review of events and actions taken to implement changes in business practices in providing the services covered by this agreement.

If, at the State's discretion the Security Incident was due to the actions or inactions of the Consultant and at the Consultant's expense the Consultant will use a credit monitoring service, call center, forensics company, advisors, or public relations firm whose services are acceptable to the State. At the State's discretion the Consultant shall offer 2 years of credit monitoring to each person whose data was compromised. The State will set the scope of any investigation. The State can require a risk assessment for which the Consultant, the State will mandate the methodology and the scope. At the State's discretion a risk assessment may be performed by a third party at the Consultant's expense.

If the Consultant is required by federal law or regulation to conduct a Security Incident or data breach investigation, the results of the investigation must be reported to the State within twelve (12) hours of the investigation report being completed. If the Consultant is required by federal law or regulation to notify the affected parties, the State must also be notified, unless otherwise required by law.

Notwithstanding any other provision of this Agreement, and in addition to any other remedies available to the State under law or equity, the Consultant will reimburse the State in full for all costs incurred by the State in investigation and remediation of the Security Incident including, but not limited, to providing notification to regulatory agencies or other entities as required by law or contract. The Consultant shall also pay any and all legal fees, audit costs, fines, and other fees imposed by regulatory agencies or contracting partners as a result of the Security Incident.

ADVERSE EVENT
The Consultant shall notify the State Contact within 2 days if the Consultant becomes aware that an Adverse Event has occurred. An Adverse Event is the unauthorized use of system privileges, unauthorized access to State data, execution of malware, physical intrusions and electronic intrusions that may include network, applications, servers, workstations and social engineering of staff. If the Adverse Event was the result of the Consultant's actions or inactions. The State can require a risk assessment of the Consultant the State mandating the methodology to be used as well as the scope. At the State's discretion a risk assessment may be performed by a third party at the Consultant's expense. State Data is any data produced or provided by the State as well as any data produced or provided for the State by a third-party.

SOURCE CODE
Consultant hereby agrees to provide to the South Dakota Bureau of Information and Telecommunications, for safekeeping, a copy of source code developed or maintained for use by the State under the terms of this Agreement. The source code provided will be the version currently running on the State's production environment.

BROWSER
The system, site, and/or application must be compatible with vendor supported versions of Edge, Chrome, Safari, and Firefox browsers. Silverlight, QuickTime, PHP, Adobe ColdFusion and Adobe Flash will not be used in the system, site, and/or application. Adobe Animate CC is allowed if files that require third-party plugins are not required.

SECURITY OF CODE
Any code written or developed by the Consultant, and Consultant's Subcontractors, Agents, Assigns and/or Affiliated Entities must comply with the security requirements of this agreement.

SECURITY ACKNOWLEDGEMENT FORM
The Consultant will be required to sign the Security Acknowledgement form which is attached to this Agreement as Attachment J The signed Security Acknowledgement form must be submitted to the State and approved by the South Dakota Bureau of Information and Telecommunications and communicated to the Consultant by the State contact before work on the contract may begin. This form constitutes the agreement of Consultant to be responsible and liable for ensuring that the Consultant, Consultant's employee(s), and Subcontractor's, Agents, Assigns and or Affiliated Entities and all of their employee(s), participating in the work will abide by the terms of the Information Technology Security Policy- Contractor (ITSP) attached to this Agreement as Attachment K. Failure to abide by the requirements of the ITSP or the Security Acknowledgement form can be considered a breach of this Agreement at the discretion of the State. It is also a breach of this Agreement, at the discretion of the State, if the Consultant does not sign another Security Acknowledgement form covering any employee(s) and any Subcontractor's, Agents, Assigns and or Affiliated Entities employee(s), any of whom are participating in the work covered by this Agreement, and who begin working under this Agreement after the project has begun. Any disciplining of the Consultant's, Consultant's employee(s) or Subcontractor's, Agents, Assigns and or Affiliated Entities employee(s) due to a failure to abide by the terms of the Security Acknowledgement Form will be done at the discretion of the Consultant or Subcontractor's, Agents, Assigns and or Affiliated Entities and in accordance with the Consultant's or Subcontractor's, Agents, Assigns and or Affiliated Entities personnel policies. Regardless of the actions taken by the Consultant and Subcontractor's, Agents, Assigns and or Affiliated Entities, the State shall retain the right to require at its discretion the removal of the employee(s) from the project covered by this agreement.

BACKGROUND CHECKS
The State requires all employee(s) of the Consultant, Subcontractors, Agents, Assigns and or Affiliated Entities who write or modify State owned software, alter hardware, configure software of state-owned technology resources, have access to source code and/or protected personally identifiable information or other confidential information or have access to secure areas to undergo fingerprint-based background checks. These fingerprints will be used to check the criminal history records of both

the State and the Federal Bureau of Investigation. These background checks must be performed by the State with support from the State's law enforcement resources. The State will supply the finger print cards and prescribe the procedure to be used to process the finger print cards. Project plans should allow two (2) to four (4) weeks to complete this process. If work assignments change after the initiation of the project covered by this agreement so that employee(s) of the Consultant, Subcontractor's, Agents, Assigns and or Affiliated Entities will be writing or modifying State owned software, altering hardware, configuring software of state owned technology resources, have access to source code and/or protected personally identifiable information or other confidential information or have access to secure areas then, background checks must be performed on any employees who will complete any of the referenced tasks. The State reserves the right to require the Consultant to prohibit any employee, Subcontractors, Agents, Assigns and or Affiliated Entities from performing work under this Agreement whenever the State, in its sole discretion, believes that having a specific employee, subcontractor, agent assign or affiliated entity performing work under this Agreement is detrimental to the project or is considered by the State to be a security risk, based on the results of the background check. The State will provide the Consultant with notice of this determination.

INFORMATION TECHNOLOGY STANDARDS
Any service, software or hardware provided under this agreement will comply with state standards which can be found at *http://bit.sd.gov/standards/* .

ACCEPTABLE PROGRAMMING LANGUAGES
The application(s) covered in this contract are written in _To be completed when Contract is created IF software is written for the State. All applications listed will be written in C#, and use ASP.NET, MVC, UWP, or WPF.

PRODUCT SUPPORT
The State will install and operate the Consultant's product on the State's computing infrastructure. The State will not be responsible for added support costs if the Consultant determines that the Consultant is unable to meet the support commitment(s) given by the Consultant in this agreement. Any additional costs for support will be borne by the Consultant.

PRODUCT USAGE
The State cannot be held liable for any additional costs or fines for mutually understood product usage over and above what has been agreed to in this Agreement unless there has been an audit conducted on the product usage. This audit must be conducted using a methodology agreed to by the State. The results of the audit must also be agreed to by the State before the State can be held to the results. Under no circumstances will the State be required to pay for the costs of said audit.

SECURITY
The Consultant shall take all actions necessary to protect State information from exploits, inappropriate alterations, access or release, and malicious attacks.

By signing this agreement, the Consultant warrants that:

A. All Critical, High, Medium, and Low security issues are resolved. Critical, High and Medium can be described as follows:
    a. **Critical** - Exploitation of the vulnerability likely results in root-level compromise of servers or infrastructure devices.
    b. **High** - The vulnerability is difficult to exploit; however, it is possible for an expert in Information Technology. Exploitation could result in elevated privileges.
    c. **Medium** - Vulnerabilities that require the attacker to manipulate individual victims via social engineering tactics. Denial of service vulnerabilities that are difficult to set up.
    d. **Low**- Vulnerabilities identified by the State as needing to be resolved that are not Critical, High, or Medium issues.
B. Assistance will be provided to the State by the Consultant in performing an investigation to determine the nature of any security issues that are discovered or are reasonably suspected after acceptance. The Consultant will fix or mitigate the risk based on the following schedule: Critical and high risk, within 7 days, medium risk within 14 days, low risk, within 30 days.
C. State technology standards, policies, and best practices will be followed. State technology standards can be found at http://bit.sd.gov/standards/.
D. All members of the development team have been successfully trained in secure programming techniques.
E. A source code control system will be used that authenticates and logs the team member associated with all changes to the software baseline and all related configuration and build files.

F. State access to the source code will be allowed to ensure State security standards, policies, and best practices which can be found at http://bit.sd.gov/standards/.

G. The Consultant will fully support and maintain the Consultant's application on platforms and code bases (including but not limited to: operating systems, hypervisors, web presentation layers, communication protocols, security products, report writers, and any other technologies on which the application depends) that are still being supported, maintained, and patched by the applicable third parties owning them. The Consultant may not withhold support from the State for this application nor charge the State additional fees as a result of the State moving the Consultant's application to a new release of third-party technology if:

   i. The previous version of the third-party code base or platform is no longer being maintained, patched, and supported; and

   ii. The new version to which the State moved the application is actively maintained, patched, and supported.

If there are multiple versions of the applicable code base or platform(s) supported by the third party in question, the Consultant may limit their support and maintenance to any one or all of the applicable third-party code bases or platforms. If a code base or platform on which the Consultant's application depends is no longer supported, maintained, or patched by a qualified third party the Consultant commits to migrate its application from that code base and/or platform to one that is supported, maintained, and patched after the State has performed a risk assessment using industry standard tools and methods. Failure on the part of the Consultant to work in good faith with the State to secure or a timely move to supported, maintained, and patched technology will allow the State to cancel this Agreement without penalty.

LICENSE TO PERFORM SECURITY SCANNING

Before acceptance by the State the Consultant will provide the State, at a time and for duration agreeable to both parties, access to the application and underlying hardware referenced in this Agreement for security scanning activities. Any scanning performed by the State will not be considered a violation of any licensure agreements the State has with the Consultant or the Consultant has with a third-party. Scanning by the State or any third-party acting for the State will not be considered reverse engineering. If the state security scanning efforts discover security issues, the State may collaborate, at the State's discretion, with the Consultant on remediation efforts. These remediation efforts will not be considered a violation of any licensure agreements the State has with the Consultant. The State will not be charged for any costs incurred by Consultant in these remediation efforts unless agreed to by the State in advance in writing. In the event of conflicting language this clause supersedes any other language in this or any other agreement made between the State and the Consultant.

SECURITY SCANNING

The State routinely applies security patches and security updates as needed to maintain compliance with industry best practices as well as state and federal audit requirements. Consultants who do business with the State must also subscribe to industry security practices and requirements. Consultants must include costs and time needs in their proposals and project plans to assure they can maintain currency with all security needs throughout the lifecycle of a project. The State will collaborate in good faith with the Consultant to help them understand and support State security requirements during all phases of a project's lifecycle but will not assume the costs to mitigate applications or processes that fail to meet then-current security requirements.

At the State's discretion, security scanning will be performed and or security settings put in place or altered during the software development phase and during pre-production review for new or updated code. These scans and tests, initially applied to development and test environments, can be time consuming and should be accounted for in project planning documents and schedules. Products not meeting the State's security and performance requirements will not be allowed into production and will be barred from User Acceptance Testing (UAT) until all issues are addressed to the State's satisfaction. The discovery of security issues during UAT are automatically sufficient grounds for non-acceptance of a product even though a product may satisfy all other acceptance criteria. Any security issues discovered during UAT that require product changes will not be considered a project change chargeable to the State. The State urges the use of industry scanning/testing tools and recommends secure development methods are employed to avoid unexpected costs and project delays. Costs to produce and deliver secure and reliable applications are the responsibility of the Consultant producing or delivering an application to the State. Unless expressly indicated in writing, the State assumes all price estimates and bids are for the delivery and support of applications and systems that will pass security and performance testing.

SECURE PRODUCT DEVELOPMENT

By signing this agreement, the Consultant agrees to provide the following information to the State:

A. Name of the person responsible for certifying that all deliverables are secure.

B. Documentation detailing the Consultant's version upgrading process.
C. Notification process for application patches and updates.
D. List of tools used in the software development environment used to verify secure coding.
E. Based on a risk assessment, provide the State the secure configuration guidelines, specifications and requirements that describe security relevant configuration options and their implications for the overall security of the software. The guidelines, specifications and requirements must include descriptions of dependencies on the supporting platform, including operating system, web server, application server and how they should be configured for security. The default configuration of the software shall be secure.

At the State's discretion the State will discuss the security controls used by the State with the Consultant upon the Consultant signing a non-disclosure agreement.

MALICIOUS CODE

A. The Consultant warrants that the service/software contains no code that does not support an application requirement.
B. The Consultant warrants that the service/software contains no malicious code.
C. The Consultant warrants that the Consultant will not insert into the service/software or any media on which the service/software is delivered any malicious or intentionally destructive code.
D. The Consultant warrants that the Consultant will use commercially reasonable efforts consistent with industry standards to scan for and remove any malicious code from the service/software before installation. In the event any malicious code is discovered in the service/software delivered by the Consultant, the Consultant shall provide the State at no charge with a copy of the applicable service/software that contains no malicious code or otherwise correct the affected portion of the services provided to the State. The remedies in this paragraph are in addition to other additional remedies available to the State.

DENIAL OF ACCESS OR REMOVAL OF AN APPLICATION AND OR HARDWARE FROM PRODUCTION

During the life of this Agreement the application and or hardware can be denied access to or removed from production at the State's discretion. The reasons for the denial of access or removal of the application and or hardware from the production system may include but not be limited to security, functionality, unsupported third-party technologies, or excessive resource consumption. Denial of access or removal of an application and or hardware also may be done if scanning shows that any updating or patching of the software and or hardware produces what the state determines are unacceptable results. The Consultant will be liable for additional work required to rectify issues concerning security, functionality, unsupported third-party technologies, and or excessive consumption of resources if it is for reasons of correcting security deficiencies or meeting the functional requirements originally agreed to for the application and or hardware. At the discretion of the State, contractual payments may be suspended while the application and or hardware is denied access to or removed from production. The reasons can be because of the Consultant's actions or inactions. Access to the production system to perform any remedying of the reasons for denial of access or removal of the software and hardware, and its updating and or patching will be made only with the State's prior approval. It is expected that the Consultant shall provide the State with proof of the safety and or effectiveness of the remedy, update or patch proposed before the State provides access to the production system. The State shall sign a non-disclosure agreement with the Consultant if revealing the update or patch will put the Consultant's intellectual property at risk. If the remedy, update or patch the Consultant proposes is unable to present software and or hardware that meets the State's requirements, as defined by the State, which may include but not limited to security, functionality, unsupported third party technologies, to the State's satisfaction within thirty (30) days of the denial of access to or removal from the production system and the Consultant does not employ the change management process to alter the project schedule or deliverables within the same thirty (30) days then at the State's discretion the Agreement may be terminated.

MOVEMENT OF PRODUCT

The State operates a virtualized computing environment and retains the right to use industry standard hypervisor high availability, fail-over, and disaster recovery systems to move instances of the product(s) between the install sites defined with the Consultant within the provisions of resource and usage restrictions outlined elsewhere in the Agreement. As part of normal operations, the State may also install the product on different computers or servers if the product is also removed from the previous computer or server within the provisions of resource and usage restrictions outlined elsewhere in the Agreement. All such movement of product can be done by the State without any additional fees or charges by the Consultant.

USE OF PRODUCT ON VIRTUALIZED INFRASTRUCTURE AND CHANGES TO THAT INFRASTRUCTURE

The State operates a virtualized computing environment and uses software-based management and resource capping. The State retains the right to use and upgrade as deemed appropriate its hypervisor and operating system technology and related hardware without additional license fees or other charges provided the State assures the guest operating system(s) running

within that hypervisor environment continue to present computing resources to the licensed product in a consistent manner. The computing resource allocations within the State's hypervisor software-based management controls for the guest operating system(s) executing the product shall be the only consideration in licensing compliance related to computing resource capacity.

LOAD BALANCING
The State routinely load balances across multiple servers, applications that run on the State's computing environment. The Consultant's product must be able to be load balanced across multiple servers. Any changes or modifications required to allow the Consultant's product to be load balanced so that it can operate on the State's computing environment will be at the Consultant's expense.

BACKUP COPIES
The State may make and keep backup copies of the licensed product without additional cost or obligation on the condition that:

A. The State maintains possession of the backup copies.
B. The backup copies are used only as bona fide backups.

USE OF ABSTRACTION TECHNOLOGIES
The Consultant's application must use abstraction technologies in all applications, that is the removal of the network control and forwarding functions that allows the network control to become directly programmable and the underlying infrastructure to be separated for applications and network services.

The Consultant warrants that hard-coded references will not be used in the application. Use of hard-coded references will result in a failure to pass pre-production testing or may cause the application to fail or be shut down at any time without warning and or be removed from production. Correcting the hardcoded references is the responsibility of the Consultant and will not be a project change chargeable to the State. If the use of hard-coded references is discovered after User Acceptance Testing the Consultant will correct the problem at no additional cost.

LICENSE AGREEMENTS
Consultant warrants that it has provided to the State and incorporated into this Agreement all license agreements, End User License Agreements, and terms of use regarding its software or any software incorporated into its software before execution of this Agreement. Failure to provide all such license agreements, End User License Agreements (EULA), and terms of use shall be a breach of this Agreement at the option of the State. The parties agree that neither the State nor its end users shall be bound by the terms of any such agreements not timely provided pursuant to this paragraph and incorporated into this Agreement. Any changes to the terms of this Agreement or any additions or subtractions must first be agreed to by both parties in writing before they go into effect. This paragraph shall control and supersede the language of any such agreements to the contrary.

WEB AND MOBILE APPLICATIONS
The Consultant's application is required to;

A. have no code or services including web services included in or called by the application unless they provide direct, functional requirements that support the State's business goals for the application;
B. encrypt data in transport and at rest using a mutually agreed upon encryption format;
C. close all connections and close the application at the end of processing;
D. the documentation will be in grammatically complete text for each call and defined variables (Use no abbreviations and use complete sentences, for example.) sufficient for a native speaker of English with average programming skills to determine the meaning and/or intent of what is written without prior knowledge of the application.
E. have no code not required for the functioning of application;
F. have no "back doors", a back door being a means of accessing a computer program that bypasses security mechanisms, or other entries into the application other than those approved by the State;
G. permit no tracking of device user's activities without providing a clear notice to the device user and requiring the device user's active approval before the application captures tracking data;
H. have no connections to any service not required by the functional requirements of the application or defined in the project requirements documentation;
I. fully disclose in the "About" information that is the listing of version information and legal notices, of the connections made, permission(s) required, and the purpose of those connections and permission(s);

J. ask only for those permissions and access rights on the user's device that are required for the defined requirements of the Consultant's application;
K. access no data outside what is defined in the "About" information for the Consultant's application;
L. your web site application produced for the State must conform to Web Content Accessibility Guidelines 2.0;
M. any website developed for the State and hosted by the State must have a Single Sign On capability with the State's other websites; and
N. any application to be used on a mobile device must be password protected.

The Consultant is required to disclose all:
A. functionality;
B. device and functional dependencies;
C. third party libraries used;
D. methods user data is being stored, processed or transmitted;
E. methods used to notify the user how their data is being stored, processed and or transmitted;
F. positive actions required by the user to give permission for their data to be stored, processed and or transmitted;
G. methods used to record the user's response(s) to the notification that their data is being stored, processed and or transmitted;
H. methods used to secure the data in storage, processing or transmission; and
I. forms of authentication required for a user to access the application or any data it gathers stores, processes and or transmits;
J. methods used to create and customize existing reports;
K. methods used to integrate with external data sources;
L. methods used if integrates with public cloud provider;
M. methods and techniques used and the security features that protect data, if a public cloud provider is used; and
N. formats the data and information uses.

If the application does not adhere to the requirements given above or the Consultant has unacceptable disclosures, at the State's discretion, the Consultant will rectify the issues at no cost to the State.

INTENDED DATA ACCESS METHODS
The Consultant's application will not allow a user, external to the State's domain, to bypass logical access controls required to meet the application's functional requirements. All database queries using the Consultant's application can only access data by methods consistent with the intended business functions.
If the State can demonstrate the application flaw, to the State's satisfaction, then the Consultant will rectify the issue, to the State's satisfaction, at no cost to the State

APPLICATION PROGRAMMING INTERFACE
Consultant documentation on application programming interface must include a listing of all data types, functional specifications, a detailed explanation on how to use the Consultant's application programming interface and tutorials. The tutorials must include working sample code.

ACCESS TO SOURCE AND OBJECT CODE
The consultant will provide access to source and object code for all outward facing areas of the system where information is presented, shared, or received whether via browser based access and programmatic-based access including but not limited to application program interfaces (APIs) or any other access or entry point accessible via the world wide web, modem, or other digital process that is connected to a digital network, radio-based or phone system.

OFFSHORE SERVICES
The Consultant will not provide access to State data to any entity or person(s) located outside the continental United States that are not named in this Agreement without the written permission of the State. This restriction also applies to disaster recovery; any disaster recovery plan must provide for data storage entirely within the continental United States.

MULTIFACTOR AUTHENTICATION
The Consultant's and the Consultant's subcontractors will not access the State's network except through the State's Multifactor Authentication process. For purposes of remote access to the State systems on the State's domain, the Consultant will adhere to the State's requirements for Multifactor Authentication upon receipt of notification from the State that such requirements have been implemented. The Consultant will also require adherence to the State's requirements by any of the Consultant's officers, employees, subcontractors, agents, assigns, and affiliated entities who will have remote access to State

systems on the State's domain. The State's requirements for Multifactor Authentication are set forth in the State's Information Technology Security Policy, which is attached as Appendix.

CONSULTANT'S SOFTWARE LICENSES

The Consultant must disclose to the State the license(s) for any third-party software and libraries used by the Consultant's product(s) ((and/or) in the project by the Consultant) covered under this agreement if the State will not be the license(s) holder. The Consultant is required to provide copies of the license(s) for the third-party software and libraries to the State. No additional software and libraries may be added to the project after the contract is signed without notifying the State and providing the licenses of the software and libraries. Open source software and libraries are also covered by this clause. Any validation of any license(s) used by the Consultant to fulfil the Consultant's commitments agreed to in this agreement is the responsibility of the Consultant, not the State.

CONSULTANT TRAINING REQUIREMENTS

The Consultant, Consultant's employee(s), and Consultant's Subcontractors, Agents, Assigns, Affiliated Entities and their employee(s), must successfully complete, at the time of hire and annually thereafter, a cyber-security training program. The training must include but is not limited to: i) Legal requirements for handling data, ii) Media sanitation, iii) Strong password protection, iv) Social engineering, or the psychological manipulation of persons into performing actions that are inconsistent with security practices or that cause the divulging of confidential information, and v) Security incident response.

DATA SANITIZATION

At the end of the project covered by this Agreement the Consultant, and Consultant's Subcontractors, Agents, Assigns and/or Affiliated Entities shall return the State's data and/or securely dispose of all State data in all forms, this can include State data on media such as paper, punched cards, magnetic tape, magnetic disks, solid state devices, or optical discs. This State data must be permanently deleted by either purging the data or destroying the medium on which the State data is found according to the methods given in the most current version of NIST 800-88. Certificates of Sanitization for Offsite Data (See bit.sd.gov/vendor/default.aspx for copy of certificate) must be completed by the Consultant and given to the State Contact. The State will review the completed Certificates of Sanitization for Offsite Data. If the State is not satisfied by the data sanitization then the Consultant will use a process and procedure that does satisfy the State. The only exceptions are when the State Data must be maintained after the project is completed for legal reasons or the State data is on a backup medium where the State data cannot be separated from other data. If the state data cannot be sanitized for these reasons, then the Consultant must encrypt the data to at least 256 AES with SHA 2 or SHA 256 hashing and maintain the medium in a facility that meets the security requirements of the most current version of NIST 800-53 or IRS 1075 whichever is relevant.
This contract clause remains in effect for as long as the Consultant, and Consultant's Subcontractors, Agents, Assigns and/or Affiliated Entities have the State data, even after the Agreement is terminated or the project is completed.

BANNED HARDWARE

The Consultant will not provide to the State any computer hardware or video surveillance hardware, or any components thereof, or any software that was manufactured, provided, or developed by a covered entity. As used in this paragraph, "covered entity" means the following entities and any subsidiary, affiliate, or successor entity and any entity that controls, is controlled by, or is under common control with such entity: Kaspersky Lab, Huwaei Technologies Company, ZTE Corporation, Hytera Communications Corporation, Hangzhou Hikvision Digital Technology Company, Dahua Technology Company, or any entity that has been identified as owned or controlled by, or otherwise connected to, People's Republic of China. The Consultant will immediately notify the State if the Consultant becomes aware of credible information that any hardware, component, or software was manufactured, provided, or developed by a covered entity.

USE OF PORTABLE DEVICES

The Consultant shall prohibit its employees, agents, affiliates and subcontractors form storing State data on portable devices, including personal computers, except for devices that are used and kept only at the Consultant's data center(s). All portable devices used for storing State Data must be password protected and encrypted.

REMOTE ACCESS

The Consultant shall prohibit its employees, agents, affiliates and subcontractors from accessing State data remotely except as necessary to provide the services under this Agreement and consistent with all contractual and statutory requirements. The accounts used for remote access cannot be shared accounts and must include multifactor authentication.

SOFTWARE LICENSE

The State grants Contractor a nonexclusive, worldwide, revocable, fully paid, nontransferable license to all code provided to the Contractor and all modifications to the licensed code, which becomes property of the State, pursuant to this Agreement. The license rights granted in this Agreement will continue so long as the Parties are under a contract regarding the licensed code.

The State grants the Contractor the right to

- use the licensed code for only the State's benefit pursuant to this Agreement;
- make as many copies of the licensed code as necessary to fulfill its obligations under this Agreement;
- modify the licensed code pursuant to the terms of this Agreement;
- publicly perform the licensed code, if applicable; and
- publicly display the licensed code, if applicable.

The Contractor is not granted the following rights and is prohibited from doing the following:

- creating derivative works from the licensed code;
- distributing the licensed code; and
- sublicensing the licensed code.

Copies of the licensed code created or transferred pursuant to this Agreement are licensed to the Contractor, not sold. Customer receives no title to or ownership of any copy or of the licensed code itself. Furthermore, Contractor receives no rights to the licensed code other than those specifically granted in this Agreement.

CONSULTANT ELECTION NOT TO RENEW CONTRACT OR TO INCREASE FEES

The Consultant is obligated to give the State one hundred and eighty (180) days written notice in the event the Consultant intends not to renew the contract or intends to raise any fees or costs associated with the Consultant's products or services in a subsequent contract unless such fees or costs have previously been negotiated and included in this contract.

DATA LOCATION

The Consultant shall provide its services to the State as well as storage of State data solely from data centers in the continental United States. The Consultant will not allow any State to be provided to or accessed by any entity outside the continental United States. This restriction includes but is not limited to Consultant's employees and contractors. This restriction also applies to disaster recovery; any disaster recovery plan must provide for data storage entirely within the continental United States. The Consultant shall not allow its employees or contractors to store State data on portable devices, including personal computers, except for devices that are used and kept only at its data centers. The Consultant shall permit its personnel and contractors to access State data remotely only as required to provide technical support or to fulfill the terms of this Agreement the Consultant's personnel may access the State data remotely. If the State's data remotely accessed is legally protected data or considered sensitive by the State, then:

i. The device used must be password protected;
ii. Multifactor Authentication must be used
iii. The data is encrypted to at least AES 256 both in transit and in storage;
iv. Data is not put onto mobile media;
v. No non-electronic copies are made of the data;
vi. The Consultant maintains a log on what data was accessed, when it was accessed, and by whom it was accessed;

The State's Data Sanitization policies are followed when the data is no longer needed on the device used to access the data remotely.

DATA PROTECTION

Protection of personal privacy and data shall be an integral part of the business activities of the Consultant to ensure there is no inappropriate or unauthorized use of State's data at any time. To this end, the Consultant shall safeguard the confidentiality, integrity and availability of State's data and comply with the following conditions:

A. The Consultant shall implement and maintain appropriate administrative, technical and organizational security measures to safeguard against unauthorized access, disclosure or theft of Personally Identifiable Information (PII), data protected under the Family Educational Rights and Privacy Act (FERPA), Protected Health Information (PHI), Federal Tax Information (FTI) or any information that is confidential under state law. Such security measures shall be in accordance with recognized industry practice and not less protective than the measures the Consultant applies to its own non-public data.

B. At no time shall any data that either belong to or are intended for the use of the State or its officers, agents or employees — be copied, disclosed or retained by the Consultant or any party related to the Consultant for subsequent use in any transaction that does not include the State.

C. The Consultant will not use such data for the Consultant's own benefit and, in particular will not engage in data mining of State's data or communications, whether through automated or manual means, except as specifically and expressly required by law or authorized in writing by the State through a State employee or officer specifically authorized to grant such use of State data.

INDEPENDENT AUDIT

The Consultant will disclose any independent audits that are performed on any of its systems. The systems included under this requirement are the Consultant's data center, ___ (Or) servers. This information on an independent audit(s)-shall be provided to the State in any event, whether the audit or certification process is successfully completed or not. The audit shall also be disclosed if the audit process did not result in a positive outcome. The Consultant will provide a copy of the findings of the audit(s) to the State.

NON-DISCLOSURE AND SEPARATION OF DUTIES

The Consultant shall enforce separation of job duties and require non-disclosure agreements of all staff that have or can have access to State data or the hardware that State data resides on. The Consultant will limit staff knowledge to those staff who duties that require them to have access to the State's data or the hardware the State's data resides on.

BUSINESS CONTINUITY AND DISASTER RECOVERY

The Consultant shall provide a business continuity and disaster recovery plan upon request and ensure that the State's Recovery Time Objective (RTO) of To Be Determined and Recovery Point objective (RPO) of To Be Determined is met. For purposes of this contract, a "Disaster" shall mean any unplanned interruption of the operation of or inaccessibility to the Consultant's service in which the State, using reasonable judgment, requires relocation of processing to a recovery location. The State shall notify the Consultant as soon as possible after the State deems a service outage to be a Disaster.

EXTRACTION OF DATA

Upon notice of termination by the Consultant or upon reaching the end of the term, any information stored in repositories not hosted on the State's infrastructure shall be extracted in a format to enable to State to load the information onto\into repositories. If this is not possible the information metadata, including data structure descriptions and data dictionary, and data will be extracted into a text file format and returned to the State. Upon the effective date of the termination of the agreement the State again requires that State applications that store information to repositories not hosted on the State's infrastructure require the Consultant before termination (whether initiated by the State or the Consultant) to extract the State's information such that the state is able to load the information onto or into repositories listed in the State's standards. If the information cannot be extracted in a format that allows the information to be loaded onto or into the State's Standard repositories the information (metadata (data structure descriptions) and data) will be extracted into a text file format and returned to the State. The Consultant recognizes and agrees that the State cannot enter into an agreement providing for hosting of any of its data on the Consultant's servers and networks without provisions protecting its ability to access and recover its data in a usable, non-proprietary format in the event of termination of this contract with sufficient time to convert that data and the business functions provided by the Consultant to another system and Consultant.

FACILITIES INSPECTION

The Consultant grants authorized State and/or federal personnel access to inspect their systems, facilities, work areas, contractual relationships with third parties involved in supporting any aspects of the hosted system, and the systems that support/protect the hosted system. This access will be granted on 24-hour notice. Such personnel will be limited to staff authorized by the State or the federal government to audit the system, and representatives of the state entity that funds the hosting. The State accepts that access will be arranged with an escort, and the Consultant commits that the escort will have the access and authority to provide physical access to facilities, answer appropriate questions, and provide requested documentation, including but not limited to executed contract terms, operating procedures, records of drills and tests, evidence of background checks, security logs, and any other items required by State or federal audit requirements or as deemed by the State to be required to demonstrate the Consultant is complying with all contract terms.

HOST FACILITY PHYSICAL SECURITY

The Consultant will provide documentation and, at the discretion of the State, allow for on-site inspections as needed to demonstrate that all facilities supporting the application have adequate physical security. This includes, at a minimum, centrally administered electronic locks that control entry and exit from all rooms where the hosted system resides. Any door

security system must either be connected to the building's power backup system as defined elsewhere or have internal battery power sufficient to last 24 hours in normal usage. Security events for the physical access system must be logged and the logs stored electronically in a secure location in a non-changeable format and must be searchable. Retention on the logs must be not less than 7 years. Log entries must be created for at least: successful entry and exit (indicating whether the access was to enter or exit the room) as well as all security related events such as, doors left open more than 30 seconds, forced entries, failed entry attempts, repeat entries without exit, repeat exits without entry, attempts to access doors for which access was not authorized. The Consultant agrees to provide, at the State's request, full access to search the security logs for any access or security events related to any and all rooms and physical locations hosting the State's system.

REDUNDANT POWER AND COOLING TO ALL HARDWARE
The Consultant will provide documentation and, at the discretion of the State, allow for on-site inspections as needed to demonstrate all facilities supporting the application have adequate redundant power and cooling capacity to operate uninterrupted, and without the need to refuel generators, for not less than 24 hours in the event the local external power fails.

UPS BACKUP
The Consultant will provide documentation and, at the discretion of the State, allow for on-site inspections as needed to demonstrate that all facilities supporting the application have adequate UPS power to carry the systems for not less than 10 minutes, and to protect the system from power fluctuations including, but not limited to, surge, spikes, sags, and instability.

RIGHTS AND LICENSE IN AND TO STATE DATA
The parties agree that between them, all rights including all intellectual property rights in and to State's data shall remain the exclusive property of the State, and that the Consultant has a limited, nonexclusive license to use these data as provided in this Agreement solely for the purpose of performing its obligations hereunder. This Agreement does not give a party any rights, implied or otherwise, to the other's data, content, or intellectual property, except as expressly stated in the Agreement.

CESSATION OF BUSINESS
The Consultant will notify the State of impending cessation of its business or that of a tiered provider and the Consultant's contingency plan. This plan should include the immediate transfer of any previously escrowed assets and data and State access to the Consultant's facilities to remove or destroy any State-owned assets and data. The Consultant shall implement its exit plan and take all necessary actions to ensure a smooth transition of service with minimal disruption to the State. The Consultant will provide a fully documented service description and perform and document a gap analysis by examining any differences between its services and those to be provided by its successor. The Consultant will also provide a full inventory and configuration of servers, routers, other hardware, and software involved in service delivery along with supporting documentation, indicating which if any of these are owned by or dedicated to the State. The Consultant will work closely with its successor to ensure a successful transition to the new equipment, with minimal downtime and impact on the State, all such work to be coordinated and performed in advance of the formal, final transition date.

SERVICE LEVEL AGREEMENTS
The Consultant warrants that all services will be performed in a professional and workmanlike manner consistent with industry standards reasonably applicable to such services. The Consultant further warrants that the services will be operational at least 99.99% of the time in any given month during the term of this Agreement. In the event of a service outage, the Consultant will:

A. Promptly and at the Consultant's expense, use commercial best efforts to restore the services as soon as possible, and

B. Unless the outage was caused by a Force Majeure event refund or credit the State, at the State's election, the pro-rated amount of fees corresponding to the time Services were unavailable or $100 US funds per incident, whichever is the greater amount. For the purpose of this agreement, an incident, regardless of time required to return to online position and whether re-keying of data is necessary to return, is defined as any significant reduction in the availability of hosted services lasting more than one minute or resulting in data loss, rework, or occurring more than 3 times in a 24-hour time period. For example, being forced offline no more than twice in 24 hours would not be an incident if the user could get back online within 60 seconds and continue work where he or she left off. Being forced off-line 3 times in a day would be an incident, regardless. Being forced off-line once in a 24-hour period of time, however, that resulted in the user having to rekey data that was lost would be an incident. Entering User authentication to log on shall not be considered data entry.

The Consultant will provide the State with seven days prior notice of scheduled downtime in the provision of services for maintenance or upgrades. To the extent possible, the Consultant will schedule downtime during times of ordinarily low use

by the State. In the event of unscheduled or unforeseen downtime for any reason, except as otherwise prohibited by law, the Consultant will promptly notify the State and respond promptly to the State's reasonable requests for information regarding the downtime.

LEGAL REQUESTS FOR DATA
Except as otherwise expressly prohibited by law, the Consultant will:

A. Immediately notify the State of any subpoenas, warrants, or other legal orders, demands or requests received by the Consultant seeking State data maintained by the Consultant;

B. Consult with the State regarding its response;

C. Cooperate with the State's requests in connection with efforts by the State to intervene and quash or modify the legal order, demand or request; and

D. Upon the State's request, provide the State with a copy of both the demand or request and its proposed or actual response.

EDISCOVERY
The Consultant shall contact the State upon receipt of any electronic discovery, litigation holds, discovery searches, and expert testimonies related to, or which in any way might reasonably require access to the data of the State. The Consultant shall not respond to service of process, and other legal requests related to the State without first notifying the State unless prohibited by law from providing such notice.

DATA RETENTION AND DISPOSAL
A. The Consultant will use commercially reasonable efforts to retain data in an End User's account until the End User deletes them, or for an alternate time period mutually agreed by the parties.

B. Using appropriate and reliable storage media, the Consultant will regularly back up State's data and retain such backup copies for a minimum of three years.

C. The Consultant will retain logs associated with End User activity for a minimum of three years, unless the parties mutually agree to a different period.

MULTI-TENANT ARCHITECTURE LOGICALLY/PHYSICALLY SEPARATED TO ENSURE DATA SECURITY
The Consultant will provide documentation and, at the discretion of the State, allow for on-site inspections as needed to demonstrate that all facilities supporting the application have adequate safeguards to assure that needed logical and physical separation is in place and enforced to insure data security, physical security, and transport security.

ACCESS ATTEMPTS
All access attempts, whether failed or successful, to any system connected to the hosted system which can access, read, alter, intercept, or otherwise impact the hosted system or its data or data integrity shall be logged by the Consultant. For all systems, the log must include at least: log-in page used, username used, time and date stamp, incoming IP for each authentication attempt, and the authentication status, whether successful or not. Logs must be maintained not less than 7 years in a searchable database in an electronic format that is un-modifiable. At the request of the state, access must be granted to search those logs as needed to demonstrate compliance with the terms of this contract, and any and all audit requirements related to the hosted system.

PASSWORD POLICIES
Password policies for all Consultant employees will be documented annually and provided to the state to assure adequate password protections are in place. Logs and administrative settings will be provided to the state on request to demonstrate such policies are actively enforced. The process used to reset a password must include security questions or Multifactor Authentication.

ANNUAL RISK ANALYSIS
The Consultant will conduct a risk analysis annually or when there has been a significant system change. The Consultant will provide verification to the State Contact upon request that the risk analysis has taken place. At a minimum the risk analysis will include a review of the:

(i) Penetration testing of the Consultant's system.
(ii) Security policies and procedures.
(iii) Disaster recovery plan.
(iv) Security incident plan.
(v) Business Associates Agreements.
(vi) Inventory of physical systems, devices and media that store or utilize ePHI for completeness.

If the risk analysis provides evidence of deficiencies a risk management plan will be produced. A summary of the risk management plan will be sent to the State Contact. The summary will include completion dates for the plan's milestones. Updates on the risk management plan will be sent to the State Contact upon request.

WEBSITE PERFORMANCE REPORT

The Consultant will provide to the State reports on the performance of the website being hosted by the Consultant or for the website if hosted by a third party for the Consultant. These reports must be produced by the Consultant on demand as well as a Third-party Hosting service. The reports will be in .cvs with a mutually agreed to format and at the State's discretion in an unprocessed format. The metrics in the reports will include i) The total number of visits to the website, ii) The average time the website takes to load, and iii) the average length of time a transaction takes on the website. The measurements should be equal to or better than:

- The average time the website takes to load is _____.
- The average length of time a transaction take is _____.

ACCESS TO STATE DATA

Unless this Agreement is terminated, State access to State data amassed under the project covered by this Agreement will not be hindered if there is a:

i) Contract dispute between the parties to this Agreement.
ii) There is a billing dispute between the parties to this Agreement.
iii) The Consultant merges with or is acquired by another company.

The Consultant will also maintain all security requirements of the State as well as any disaster recovery commitments made under this Agreement.

SUSPENSION OF SERVICES

The State may suspend, or terminate, or direct the Consultant to suspend or terminate, an End User's access to services in accordance with the State's policies an End User being in breach of terms of service. The State will assume sole responsibility for any claims made by End Users regarding the State's suspension/termination or directive to suspend/terminate such service. The Consultant may suspend access to services to an End User(s) immediately in response to an act or omission that reasonably appears to jeopardize the security or integrity of the Consultant's services or the network(s) or facilities used to provide the services. Suspension will be to the minimum extent, and of the minimum duration, required to prevent or end the security issue. The Consultant may suspend the State's access to services if, after at least 30 days' written notice to the State and subsequent good-faith, commercially reasonable efforts to resolve the matter with the State to the parties' mutual satisfaction, the State remains in material breach of this Agreement. The suspension will be lifted immediately when the breach is cured. The Consultant may suspend access to services by an End User in response to a material breach by End User of any terms of use he or she has agreed to in connection with receiving the services. The Consultant will notify the State of any suspension of End User access to services.

THIRD PARTY HOSTING

If the Consultant has the State's data hosted by another party the Consultant must provide the State, the name of this party. The Consultant must provide the State with contact information for this third party and the location of their data center(s). The Consultant must receive from the third party written assurances that the state's data will reside in the continental United States at all times and provide these written assurances to the State. This restriction includes the data being viewed or accessed by the third-party's employees or contractors. If during the term of this agreement the consultant changes from the Consultant hosting the data to a third-party hosting the data or changes third-party hosting provider, the Consultant will provide the State with one hundred and eighty (180) days' advance notice of this change and at that time provide the state with the information required above.

SECURING OF DATA

All facilities used to store, and process State's data will employ industry best practices, including appropriate administrative, physical, and technical safeguards, to secure such data from unauthorized access, disclosure, alteration, and use. Such measures will be no less protective than those used to secure the Consultant's own data of a similar type, and in no event less than commercially reasonable in view of the type and nature of the data involved. Without limiting the foregoing, the Consultant warrants that all State's data will be encrypted in transmission (including via web interface) and storage at no less than AES256 level encryption with SHA256 or SHA2 hashing.

SECURITY PROCESSES
The Consultant shall disclose its non-proprietary security processes and technical limitations to the State such that adequate protection and flexibility can be attained between the State and the Consultant. For example: virus checking and port sniffing.

IMPORT AND EXPORT OF DATA
The State shall have the ability to import or export data piecemeal or in entirety at its discretion without interference from the Consultant. This includes the ability for the State to import or export data to/from other Consultants.

SCANNING AND AUDIT AUTHORIZATION
The Consultant will provide the State at no cost and at a date, time and for duration agreeable to both parties, authorization to scan and access to a test system containing test data for security scanning activities. The system and data provided to the State by Consultant for testing purposes will be considered a test system containing test data. The State will not scan any environment known by the State to be a production environment at the time the scan is performed by the State. Consultant provides their consent for the State or any third-party acting for the State to scan the systems and data provided as the State wishes using any methodology that the State wishes. Any scanning performed by the State will not be considered a violation of any licensure agreements the State has with the Consultant or that the consultant has with a third-party.

The Consultant will also allow the State at the State's expense, not to include Consultant's expenses, to perform up to two security audit and vulnerability assessments per year to provide verification of Consultant's IT security safeguards for the system and its data. The State will work with the Consultant to arrange the audit at a time least likely to create workload issues for the Consultant and will accept scanning a test or UAT environment on which the code and systems are a mirror image of the production environment.

Scanning by the State or any third-party acting for the State will not be considered reverse engineering. If the State's security scans discover security issues the State may collaborate, at the State's discretion with, the Consultant on remediation efforts. These remediation efforts will not be considered a violation of any licensure agreements between the State and Consultant. In the event of conflicting language this clause supersedes any other language in this, or any other agreement made between the State and the Consultant.

The Consultant agrees to work with the State to rectify any serious security issues revealed by the security audit and or security scanning. This includes additional security audits and security scanning that shall be performed after any remediation efforts to confirm the security issues have been resolved and no further security issues exist. If the Consultant and the State agree that scanning results cannot be achieved that are acceptable to the State, then the State may terminate the Agreement without further obligation.

SYSTEM UPGRADES
Advance notice of 30 days shall be provided the State of any major upgrades or system changes the Consultant will be implementing unless the changes are for reasons of security. A major upgrade is a replacement of hardware, software or firmware with a newer or improved version, in order to bring the system up to date or to improve its characteristics. The State reserves the right to postpone these changes unless the upgrades are for security reasons. The State reserves the right to scan the Consultant's systems for vulnerabilities after a system upgrade. These vulnerability scan can include penetration testing of a test system at the State's discretion.

PASSWORD PROTECTION
The website(s) and or service(s) that will be hosted by the Consultant for the State will be password protected. If the Consultant provides the user with a preset or default password that password cannot include any Personally Identifiable Information, data protected under the Family Educational Rights and Privacy Act, Protected Health Information, Federal Tax Information or any information defined under state statute as Confidential Information or fragment thereof.

MOVEMENT OF PROTECTED STATE DATA

Any State data that is protected by Federal or State statute or requirements or by industry standards must be kept secure. When protected State data is moved to any of the Consultant's production or non-production systems, security must be maintained. The Consultant will ensure that that data will at least have the same level of security as it had on the State's environment. The State's security policies can be found in the Information Technology Security Policies (ITSP).

BANNED SERVICES

The Consultant warrants that any hardware or hardware components used to provide the services covered by this Agreement were not manufactured by Huawei Technologies Company or ZTE Corporation, or any subsidiary or affiliate of such entities. Any company considered to be a security risk by the government of the United States under the International Emergency Economic Powers Act or in a United States appropriation bill will be included in this ban.

MULTIFACTOR AUTHENTICATION FOR HOSTED SYSTEMS

If the Consultant is hosting on their system or performing Software as a Service where there is the potential for the Consultant and/or the Consultant's subcontractor to see protected State data, then Multifactor Authentication (MFA) must be used to before this data can be accessed. The Consultant's MFA, at a minimum must adhere to the requirements of *Level 3 Authentication Assurance for MFA* as defined in NIST 800-63.

ATTACHMENT B – Functional Requirements Matrix

This must be downloaded as the Excel document
RFP_2814_Attachment_B -Functional_Requirements_Matrix.xls

INSTRUCTIONS FOR COMPLETING THE MATRIX

For each requirement listed in the Main worksheet, Offerors will populate with an "x" **one** of the following columns - O, P, Q, R - based on how its proposed solution meets that requirement.

For purposes of determining how to populate these columns, Offerors will apply the following definitions:

- Configuration: a software application's features or behavior can be changed through the use of functionality, tools and/or utilities native to/built into the software application, i.e. without the need for custom programming/coding.

- Customization: a feature, extension or modification of a software application's feature that requires custom programming/coding.

Offerors are encouraged to make use of Column S - EXPLANATION/ELABORATION - to provide as much detail as deemed appropriate on how the proposed solution meets, or does not meet, a particular requirement.

ATTACHMENT C – Technical Requirements Matrix

This must be downloaded as the Excel document
RFP_2814_Attachment_C_Tech_Requirements_Matrix.xlsx

Instructions:

For each requirement listed in this worksheet, the Offeror will enter "Yes" or "No" in Column C, based on how its proposed solution meets the requirement.

For requirements that the Offeror does not meet currently, the Offeror will use Column D to elaborate on the level of effort and time require to achieve compliance.

ATTACHMENT C – Technical Requirements Matrix

This must be downloaded as the Excel document
RFP_2814_Attachment_C_Tech_Requirements_Matrix.xlsx

ATTACHMENT D – Interface Requirements Matrix

This must be downloaded as the Excel document
RFP_2814_Attachment_D-Interface_Requirements.xlsx

INSTRUCTIONS FOR COMPLETING THE MAIN WORKSHEET

- Offerors MUST COMPLETE the Main worksheet.

For each requirement listed in these worksheets, an Offeror will populate column J **with a "Y" or an "N"** based on the manner in which the Offeror can address that interface.

For purposes of determining how to populate column J, Offerors will apply the following rule:

- An Offeror will enter "Y" in column J ONLY IF IT WILL NOT have to develop, test and implement custom coding/programming to enable the interface. Otherwise it must enter "N" in column J.

An Offeror is encouraged to make use of Column K - EXPLANATION/ELABORATION - to provide as much detail as deemed appropriate on how it proposes to address each interface.

ATTACHMENT E – Mandated Report Requirements Matrix

This must be downloaded as the Excel document
RFP_2814_ Attachment_E-Mandated_Report_Requirements.xlsx

This attachment contains specifications for state reports (for publication) or federally mandated reports for which data captured in the Office of Licensing and Accreditation (OLA) Management Information System (MIS) is required. The creation of the reports may not be the responsibility of OLA; however in all of the instances noted in the Main worksheet OLA will be required to supply the data for the reports.

INSTRUCTIONS FOR COMPLETING THE MATRIX

For each required form listed in the Main worksheet, an Offeror will populate column I **with a "Y" or an "N"** based on the manner in which the Offeror can address that report in its proposed solution.

For purposes of determining how to populate column I, Offerors will apply the following rule:

- An Offeror will enter "Y" in column I ONLY IF IT WILL NOT have to develop, test and implement custom coding/programming to create the report or supply the data required for the report. Otherwise it must enter "N" in column I.

An Offeror is encouraged to make use of Column J - EXPLANATION/ELABORATION - to provide as much detail as deemed appropriate on how it proposes to address each required form.

ATTACHMENT F: Information System Management Requirements

The Contractor shall implement, operate, maintain, and provide end user support to information systems essential to meeting the information system functional and technical requirements as well as the associated performance requirements outlined in this RFP. To that end, the Contractor shall conduct information system design, development (configuration and/or customization, as defined in this document), testing, deployment, documentation, knowledge transfer, and post-implementation activities as outlined in this document. The Contractor shall complete these activities, hereafter referred to in the aggregate as **Information System Management** activities, according to expectations which will be documented in the Implementation Plan deliverable and the Service Level Agreement between the Contractor and the State.
The State expects that, as an integral part of conducting Information System Management activities, the Contractor shall collaborate with the State in the development of information system specifications, including but not limited to specifications for interfaces between State systems and Contractor systems, testing protocols, and data migration and conversion rules and algorithms. the State also expects that the Contractor shall collaborate with the State in the development of the Implementation Plan and, subsequently, in the development of the Operations, Maintenance, and Support Services Plan. Additionally, the State expects that the Contractor shall collaborate with the Department of Social Services (DSS) in the management of the information system's implementation. To that end, the Contractor shall adopt processes and tools already developed and employed by DSS to manage the portfolio of DSS information system projects. The use of these processes and tools may apply to any of the activities described in this document.

1. **Project Initiation:** The Contractor will have a repeatable, tested approach for kicking off the implementation of the MIS. The aim of Project Initiation is to ensure that the State and relevant stakeholders understand and approve of the Contractor's approach to implementation, communications, documentation review and progress tracking throughout the lifespan of the project. Project Initiation will include the following deliverables.

Deliverables:

a. **Project Kickoff Protocol and Materials Package** – By a mutually agreed upon date, the Contractor will provide a documented protocol for project initiation and a package of materials that, once customized, would be used in meetings, presentations and other project kickoff activities.

b. **Implementation Plan** - By a mutually agreed upon date, the Contractor will produce a baseline Implementation Plan. The Contractor's Implementation Plan will demonstrate that the Contractor has a thorough understanding of the Scope of Work and what must be done to satisfy the project requirements and will reflect the State's desire for how the implementation will be effected. The Implementation Plan must include detail sufficient to give the State an understanding of how the Contractor intends to:

- Manage the work;
- Guide work execution;
- Utilize Contractor resources for certain project activities;
- Rely on State resources for certain project activities;
- Document assumptions and decisions;
- Facilitate communication among stakeholders; and
- Define key management review as to content, scope, and schedule.

The Contractor's Implementation Plan shall be constructed in accordance with industry standards, accepted project management principles outlined in the Project Management Body of Knowledge (PMBOK) from the Project Management Institute (PMI), or acceptable equivalent. Additional criteria for the Implementation Plan are reflected in the following:

The Implementation Plan shall include, at a minimum: a three-level work breakdown structure; project milestones; and deliverables. Furthermore, the implementation plan must address implementation of each phase of the project. Additionally,

- The Implementation Plan shall also incorporate all locations where the Contractor proposes to perform work associated with the MIS project.
- For this project, it will be crucial to coordinate activities and resources with pertinent State staff. Thus, in its Implementation Plan the Contractor must clearly specify deliverables and dates that require BIT's

involvement for technical setup and project environments and the involvement of DSS staff in implementation activities.

- The Contractor must build, produce and maintain the project Implementation Plan in Microsoft Project or comparable project management system approved by the State.

The Implementation Plan shall describe the Contractor's process to complete each major project phase (i.e., Project Initiation; Requirement Elaboration and Specification Definition; Build: Configuration, Customization and Integration; Testing; Knowledge Transfer and Training; Data Conversion and Migration; Deployment: Cutover
and Acceptance; and Implementation Closeout). This will include the proposed project management methodology, milestone schedule, staffing plan and organizational chart.

c. Project Management and Communications Plan - By a mutually agreed upon date, the Contractor, with input from State staff, will produce a mutually agreeable Project Management and Communications Plan that defines how the project will be executed, monitored, and controlled as well as how various project stakeholders will be engaged throughout the life of the project to ensure all impacted parties are aware of project progress and are consulted as needed. Included will be:

- A list of deliverables and milestones, describing exactly what will be provided to meet those deliverables
- Metrics used to determine when deliverables have been met
- Project schedule associated with each deliverable

The Contractor is expected to participate in regularly scheduled on-site project management meetings and provide weekly status reports.

d. Risk Management Plan – By a mutually agreed upon date, the Contractor will produce a Risk Management Plan. The Risk Management Plan must be a forward-looking plan that describes:

- How the Contractor has already identified – based on prior experience and organizational experience - and will, during the course of the implementation, identify issues that could affect the achievement of project objectives;
- How the Contractor will systematically assess and rank the risk associated with these issues;
- How the Contractor is already pursuing or would rapidly develop and implement mitigation strategies that effectively address the risks associated with the aforementioned issues; and
- The tools the Contractor will use for tracking internal (Contractor) and external (State) issues and related risks, including both technical and non-technical issues that could affect the project deliverables, schedule and/or budget.

The State expects that, at a minimum, the plan will contain the following:

- Risk Management Approach - This section of the Risk Management Plan should provide a general description for the approach the Contractor will take to identify and manage the risks associated with the project.
- Risk Identification - This section of the Risk Management Plan should explain the process by which the risks associated with the MIS project will be identified. It should describe the method(s) for how the Contractor identifies the risks, the format in which risks are recorded, and the forum in which this process will be conducted.
- Risk Qualification and Prioritization - This section of the Risk Management Plan should describe the Contractor's approach to determining the probability and impact of each risk in order to allow the project manager to prioritize the risk avoidance and mitigation strategy. This is usually done with a risk matrix. This section should also explain how risks will be qualified and prioritized for this project
- Risk Monitoring - This section of the Risk Management Plan should discuss how the risks in the project will be actively monitored ensuring that it is continuous throughout the life of the project and includes the identification of trigger conditions for each risk and thorough documentation of the process.
- Risk Mitigation and Avoidance - Once risks have been qualified, determination must be made on how to address those risks which have the greatest potential probability and impact on the MIS project. This section of the Risk Management Plan should explain the considerations which must be made and the options available to the project manager in managing these risks.

e. Project Documentation and Collaboration Environment Design - By a mutually agreed upon date, the Contractor will produce a Project Documentation and Collaboration Environment Design document.

The Contractor's Project Documentation and Collaboration Environment Design document must describe the environment which the Contractor would set up to manage the flow of project-related documents and information and to facilitate collaboration among project team members. This environment can take the form of an online "project portal".

f. Project Status Report, Issue Log and Change Log Templates - By a mutually agreed upon date, the Contractor will produce Project Status Report, Issue Log and Change Log templates for use throughout the implementation. These documents will provide, respectively: current, valid information about the implementation's status by task; a comprehensive compendium of triaged, prioritized implementation issues for discussion with the State; and a comprehensive record of changes to solution scope, design and configuration which have been agreed to by the Contractor and the State.

2. Information System Requirement Elaboration and Specification Definition

The Contractor shall undertake requirement elaboration and specification definition activities including but not limited to design sessions/workshops with select State personnel. The aim of Requirement Elaboration and Specification Definition is to clearly outline the detailed design and configuration of the Contractor's solution information systems and identify any required customization work. This will require the discovery and documentation of current business practices, where appropriate, clarification of RFP requirements and defining specifications. This work shall include eliciting and documenting input from stakeholders to gain an understanding of user requirements and needs, work across teams to define workflows, and determine user priorities for information systems. The Contractor shall be conversant with the business environment of long-term services and supports to address potential roadblocks, challenges, and risks. A gap analysis may be required to determine the differences between current practices and proposed information system functions and features in order to formulate solutions to those gaps.
The Contractor shall complete this task in accordance with the dates set forth in the approved Implementation Plan and, throughout this task, raise any required information system modifications and interface needs.
The Contractor's solution and supporting information systems shall be implemented in a manner that allows for the evolution of operations and business practices with minimal impact and re-work. As a result of these activities, the Implementation and Deployment Plans may need to be modified. It is expected that, as part of this task, the Contractor shall engage in analysis of current-state processes and recommendations regarding changes to these processes or the engineering of entirely new processes with the goals of facilitating the information system's implementation and enabling improvements in OLA processes.

Deliverables:

a. **Requirement Elaboration and Specification Definition Protocol and Materials Package** - The Contractor shall conduct requirement elaboration and specification definition activities in accordance with its proposed protocol. The Contractor shall outline this protocol in the Requirement Elaboration and Specification Definition Protocol and Materials Package, to be completed in accordance with the dates set forth in the approved implementation plan. The protocol must simultaneously account for a phased implementation, if so specified by the State, and the need to engage stakeholders in certain requirement elaboration and specification definition activities.

b. **Functional Specification Documents –** In accordance with the dates set forth in the approved implementation plan, the Contractor shall develop Functional Specification Documents that it shall submit to the State for review in a manner prior approved by the State. These documents will provide a detailed description, from a user's perspective, of the functionality and user experience that the Contractor's solution information system will provide and how it will behave under various conditions. Functional specification documents serve multiple purposes, including:

- Configuration and, if applicable, customization instructions to developers;
- A basis for estimating configuration/customization level of effort and work duration;
- Agreement with the State on exactly what the Contractor shall build (configure and/or customize); and

- A point of synchronization for the whole project team regarding information system functionality that the Contractor shall supply.

After the State reviews and approves functional specification documents, any changes to said specifications will require the State review and approval.

c. **Requirements Traceability Matrix** - The State expects that a major deliverable of this task is a detailed functional requirements traceability matrix. The Contractor shall complete this matrix in accordance with the dates set forth in the approved implementation plan. This matrix will reflect the actual configuration required to implement the system. This matrix will be used throughout the life of the project, including acceptance testing.

d. **Data Integration/Interface Specifications Documents** - The Contractor shall document how it will exchange or accept data from other information systems and how said data shall be transmitted. These documents will elaborate on the interface in terms of format, content and transmission method. At a minimum, these documents will include:

- The concept of operations for each interface;
- Definitions of the message structure and protocols that govern the interchange of data;
- Identification of the communication paths along which the project team expects data to flow;
- A description of the data exchange format and protocol for exchange;
- Documentation of exception/error handling process
- A general description of each interface;
- Assumptions where appropriate; and
- Estimated size and frequency of data exchange.

Data Integration/Interface Specifications Documents will be completed in accordance with the dates set forth in the approved implementation plan.

3. Information System Build: Configuration, As-Needed Customization, and Integration

The Contractor shall perform information system configuration, as-needed customization and integration activities in accordance with the Implementation Plan and the outputs of the requirements elaboration and specifications definition task.

As part of this task, the Contractor shall collaborate with the State and as directed by the State, its agents in the design, development, testing, implementation and operations and maintenance of interfaces that enable the exchange of required data between the Contractor and the State. To the extent these data exchanges already have specifications, said specifications are outlined in **Attachment D: Interface Requirements**, Where the State has already developed interface specifications, the Contractor shall adopt those specifications.

Deliverables:

a. Information System Build Progress Reports and Status Reports - The Contractor will provide regular updates on project status to the State project manager and team. Such updates shall include, but not be limited to all completed or pending actions, status of deliverables, variances from implementation plan, and planned versus actual delivery dates. The State reserves the right to specify the mode and frequency of these updates after project initiation and to request updates and modifications to the mode and frequency at any time during the project.

b. Along with the State's project manager, and in accordance with the Project Management and Communications Plan, the Contractor shall participate in project briefings and supply content for communications materials that convey project status and progress to executive sponsors and key stakeholders.

3. Information System Testing

The Contractor shall demonstrate through a formal, prior-approved testing protocol that the information systems essential to meeting the operational and performance requirements outlined in this contract perform as required and appear to meet or exceed the State's functional and technical requirements. The testing protocol will incorporate all levels of testing:

unit/module, integration, performance, security and end user acceptance. The Contractor shall work with the State to develop specific written criteria for any testing that will objectively measure functional and technical requirements.
Testing will require coordination with the State to extract and validate testing results. Based on results and outcome of testing, the Contractor may need to adjust the system configuration and/or development, and retest until satisfactory results are achieved.
The State anticipates considerable collaboration with the Contractor in the construction of a comprehensive Testing Plan construction and will have a State team involved in user acceptance testing.
This Task shall be completed according to the timeline agreed upon in the Implementation Plan.
The failure of any specific portion of a test shall require that the entire test be rerun, not just the failed portion of the test.
The State determination of the Contractor's go-live readiness will be based in part on the results of information system tests, and only after designated State personnel (and designated State agents, if applicable) have reviewed documented Test Results and provided written acknowledgement that tests have been completed successfully as defined in the Testing Plan.

Deliverables:

a. Testing Plan – The Contractor shall submit a comprehensive Testing Plan to the State in accordance with the dates set forth in the approved Implementation Plan. Testing will include all software components in accordance with published functions and features, based on business scenarios and user friendliness. Interfaces will be tested based on design and business scenarios. At a minimum, the Testing Plan will incorporate unit, integration, usability, performance, interface, load, failover, security, and user acceptance tests. For each of the types of tests that will need to be performed, the Testing Plan will outline the following:

- Scope;
- Objective;
- Roles and Responsibilities;
- Test Schedule;
- Test Execution Protocol/Workflow;
- Assumptions for Test Execution;
- Constraints for Test Execution;
- Test Scripts – these must be tied to functional requirements;
- Test Data Requirements;
- Test Resource Requirements;
- Expected Results and Exit Criteria;
- Acceptance Criteria (including item pass/fail criteria);
- Issue Tracking;
- Issue Reporting;
- Testing Status Reports;
- Stage Completion Reports;
- Test Final Report Sign-Off;
- Risk Mitigation;
- Testing Facilities;
- Testing Tools;
- Issue Tracking Tools;
- Issue Severity and Priority Definition;
- Issue Reporting;
- Remediation Process; and
- Methods and Tools for Providing Test Result Information

b. Information System Test Results – The Contractor shall provide information system test results in accordance with specifications outlined in the Testing Plan.

4. Data Migration and Conversion

As a critical part of implementing the solution, the Contractor shall perform all applicable data migration and conversion tasks working in concert with the State and, if applicable, select State agents.

Deliverables:

a. Data Migration and Conversion Plan – The Contractor shall develop a Data Conversion and Migration Plan. The Plan will be produced in accordance with the dates set forth in the approved Implementation Plan. The plan must outline:

- The scope of data conversion/migration activities;
- An inventory/catalog and profile of data to be converted, if applicable;
- The approach to be followed for all data conversion and migration tasks for all applicable functional areas, including a detailing of specific subtasks, their durations and applicable dependencies;
- A list of information systems impacted;
- A list of conversion and reconciliation tools to be employed;
- An outline of conversion roles and responsibilities;
- A description of conversion resource requirements;
- The approach and methodology to data transformations;
- The approach to be followed for data cleanup;
- The approach and methodology for data classification (i.e., organization and/or tagging);
- The approach to be followed for methodology for conversion testing/validation;
- An outline of acceptance criteria; and
- The approach to providing information on the status and results of data migration and conversion subtasks.

It is expected that the Contractor shall address its approach to completing the following tasks in the Data Migration and Conversion Plan:

- Ensure database backups are in place;
- Execute data conversion routines/packages;
- Validate converted data to confirm success;
- Revert to backup if conversion fails;
- Provide the State with the results of the conversion and any exceptions;
- Work with the State to resolve nulls and non-converted data; and
- Provide post conversion support through requested ad-hoc reporting and provision of access to the pre- and post- converted data for the State confirmation analysis.

b. Data Migration and Conversion Results – The Contractor shall provide information on data migration and conversion Results in accordance with specifications outlined in the Data Migration and Conversion Plan.

5. Information System Knowledge Transfer and Training

The Contractor shall conduct select knowledge transfer and training tasks for designated State personnel, State staff end users, and other end users (e.g., Providers).
The Contractor shall discuss and reach agreement with the State on the optimal staging and provision of knowledge transfer and training tasks.
It is expected that, as part of this Task, the Contractor will provide resources with training and organizational change management (OCM) expertise and incorporate information system adoption, information system training and OCM best practices and techniques into its Information System Knowledge Transfer and Training Plan.
Deliverables:

a. Information System Knowledge Transfer and Training Plan - The Contractor shall develop and execute, in collaboration with the State, a Knowledge Transfer and Training Plan that will be approved by the State Project Manager. The plan will be completed in accordance with the dates set forth in the approved Implementation Plan and shall outline separate, detailed approaches for two distinct audiences: system administrators and end users.

For each applicable audience, the Information System Knowledge Transfer and Training Plan will include at a minimum:

- A recommended approach to knowledge transfer/training - approaches will be designed for adult learners with a variety of backgrounds, experiences, and learning styles;
- The population size and types of roles within each designated audience;
- A recommended approach to assessing acquired skills;
- An inventory of tasks, deliverables, and resources necessary to complete the knowledge transfer/training effort, including tools and documentation necessary to support the proposed effort; and
- For each method or course:
    - A course description;
    - The target audience (system administrator, end user or other);
    - Proposed goals;
    - Proposed standards;
    - The specific plan for transferring knowledge to/training relevant personnel, including State input;
    - The delivery timeframe (by phase/implementation step) with a strategy for optimally timing knowledge transfer and training activities;
    - A description of knowledge transfer and training deliverables and format (i.e., online, written documentation, course materials); and
    - A description of skill sets which should be achieved at the end of knowledge transfer/training, how knowledge transfer/training effectiveness will be measured and, if not achieved, addressed.

The Contractor's the State-approved training schedule must be closely coordinated with the State staff. Upon acceptance by the State Project Manager, the Contractor shall implement the approved Plan.

b. Training Materials Package – The Contractor shall organize and develop materials for use in knowledge transfer and training tasks as outlined in the Information System Knowledge Transfer and Training Plan. Materials shall include, if directed by the State, training guides with sufficient detail to be employed by trainers for current and future providers. Sufficient detail required equates to details needed for a "train the trainer" approach (i.e., trainers not part of Contractor organization) to delivering training for users within a particular organization in addition to materials for Contractor trainers to use directly with training participants. The State will review and approve these materials prior to their use and expects to receive final versions of training materials in hardcopy and electronic formats. The State will have full authority to edit/customize all Contractor-provided end user and system administrator training documentation.

c. End-User Manuals and Quick Reference Guides – The Contractor shall be responsible for providing sufficient reference materials and takeaway documents, such as user manuals, user guides, video tutorials, or "cheat sheets" to complement initial knowledge transfer and training activities and to provide follow-up reference material for trainees and users. The State will review and approve these materials prior to their use.

6. Information System Deployment and Acceptance

As part of implementation, an information system deployment workgroup comprised of State personnel, the Contractor, and other stakeholders as deemed applicable by the State will plan and execute the information system cutover and move to production of the Contractor's information systems, in concert with all interfaces between said

systems and information systems managed by the State or its agents. The Contractor shall manage the deployment of its information systems, whereas the State will manage the information system acceptance process as part of overall go-live readiness. Deployment tasks include facilitating relevant tasks and milestones according to schedule, ensuring effective communications amongst stakeholders, and recording and resolving incidents and Defects. Incident and Defect resolution work managed by the Contractor shall not interfere with the development of future functionality either as part of planned phases or due to Change Orders.

Deliverables:

a. Information System Deployment and Acceptance Plan – The Contractor shall provide an Information System Deployment and Acceptance Plan that details the process whereby the Contractor will move the fully configured and as-needed customized information systems that are part of the solution into production and Go Live. The Deployment and Acceptance Plan shall be produced in accordance with the dates set forth in the approved Implementation Plan.

The Deployment and Acceptance Plan will address, at a minimum:

- Deployment activities, including deployment of user documentation and online help;
- Sequencing of all deployment events;
- Deployment schedule;
- Go/No-Go Decision Points;
- Incident and Defect Resolution documentation and tracking, including Defect classification as described in **Attachment XXX, Key Performance Indicators**; and
- Cut-off schedule for legacy information systems.

b. Incident and Defect Resolution Log and Report – During the course of deployment, and through final solution acceptance, the Contractor shall maintain a document that serves as a combined log/report in which the following information is maintained:

- Recording and codification of incidents and/or problems with the solution that compromise its availability or performance: At a minimum the following information shall be captured for each incident: incident's reporting origin, a description of the incident including the incident's impact, and the codification of the incident based on potential cause(s), magnitude and resolution priority.
- Recording and codification of Defects and/or problems with the solution that limit or otherwise adversely impact its functionality: At a minimum the following information shall be captured for each Defect: Defect's reporting origin, a description of the Defect including the Defect's scope and functionality affected, and the classification of the Defect based on potential cause(s), magnitude and resolution priority.
- Resolution of incidents and Defects: At a minimum, the log/report shall capture, irrespective of reporting origin, interim and final measures taken by the Contractor (and, if applicable, the State) to resolve incidents and Defects.
- Date/time stamps for events associated with all the above.

c. Production Deployment Certification – The Contractor shall demonstrate full production deployment as articulated in the Deployment and Acceptance Plan and as further stipulated by the State as part of its plan to ascertain go-live readiness.

7. Information System Operations, Maintenance and Support Services

The Information System Operations, Maintenance and Support Services period officially begins upon the State officially declaring that the solution's implementation has been completed.

Information System Operations, Maintenance and Support Services provided by the Contractor shall ensure that:

- Contractor information systems are operated and maintained in accordance with requirements outlined in Sections 7.1 and 7.2, respectively.

- Required information system functionality is available and performs in accordance with key performance expectations as outlined in this RFP; refer to **Attachment XXX** for Key Performance Indicators (KPIs); and
- End users are properly supported, i.e., that end user inquiries about the solution are resolved in a timely manner and to the end user's satisfaction such that the end user can derive maximum benefit from said systems.

The Contractor shall provide Information System Operations, Maintenance and Support Services as outlined below for the four service categories: information system operations, information system maintenance, information security management, and information system end user support.

7.1 **Information System Operations**

Information System Operations services shall include but not be limited to:

- Information system hosting.
- Information system job management.
- Information system availability, performance and capacity monitoring.
- Information system backups. Backups must include, at a minimum, application and database backups and should be geographically collocated.
- Data administration including continuous review and assurance of data integrity and quality and appropriate classification of data and relationships across data elements.
- Availability assurance, including industry standards for protecting information security and providing for disaster recovery, and the requirements found at 45 CFR 205.50; 45 CFR, Subpart F, §§ 95.601-95.64.
- Information system documentation:
    - The Contractor shall maintain all information system documentation and relevant technical material in a form that ensures its continuous currency and suitability for review by State personnel or designees, knowledge transfer and transition support.
    - Contractor information system documentation shall be structured and maintained in a manner consistent with the current procedures and practices within BIT and the Contractor's Information System Operations, Maintenance and Support Services (OMSS) Plan deliverable described later in this subsection.
    - Contractor information system documentation shall be housed in an information repository that is prior-approved by the State for which access is unrestricted to designated the State personnel.
    - The Contractor shall conduct a documentation review session at least annually, presenting the contents of information system documentation to the State to ensure that it is accurate and complete for the intended purpose. the State reserves the right to audit and approve information system documentation.

    - All application programming interface (API) documentation shall follow OpenAPI standards.

7.2 **Information System Maintenance**

Information System Maintenance services shall include but not be limited to:

- Trouble ticket management, accessible to designated personnel from the State and other parties;
- Change order management; and
- Change management post Go Live: application updates, application releases, changes to hosting environment, changes to operating hardware and software.
-

Given the criticality of change order management to ensuring the solution continually meets State requirements, specific provisions that will govern change order management are outlined in Section 7.2.1.

7.2.1 **Change order management**

To the extent that information system functionality and technical capabilities are required that were not initially prescribed in the RFP and resulting Contract, the Contractor shall be expected to

provide additional information system engineering services to complete specific design, development and implementation tasks for information system modifications and enhancements.

Change Orders for such services will be executed as discussed, negotiated and ultimately agreed upon by the Contractor and the State. When any such Change Order is executed, the work will be considered part of the Contractor's Maintenance and Support Services. The process of executing a Change Order will involve jointly defining the work required, the Contractor providing an estimate of the time and costs involved for that particular task, and negotiation regarding scope, time and costs that results in acceptance by the State of the jointly-developed Change Order. The State will cover the cost incurred by the Contractor for work associated with a change order as mutually agreed between the Contractor and the State and, generally, in accordance with the following guidelines - specific compensation provisions will be built into each change order and will be subject to fund availability:

- The State may make an initial change order payment based on a percentage of the total change order cost in recognition of the level of effort involved to establish the scope, complexity, effort, timing, and specifications associated with the requested change.
- The State may effectuate other payments to the Contractor for change order related tasks based on milestones met.
- The State may withhold final payment for change order related tasks until after information system modifications and/or enhancements have been reviewed and deemed fully operational, in accordance with testing and compliance requirements built into the change order.

When performing development work under this section, the Contractor shall follow the project management and information system management processes set forth in preceding subsections of this Contract.

7.3 **Information System Security Management**

The Contractor shall manage the security of the solution according to standards published by BIT. Information System Security Management services shall include:

- Information system security monitoring;
- Management of information system security incidents;
- Information system security assessments that, at a minimum, incorporate periodic vulnerability assessments, penetration tests, and security risk assessments;
- Information system security and risk management plan updates;
- Security system updates; and
- Ensuring that, for information maintained in and accessible via the solution, access to said information and the integrity thereof are protected in accordance with 45 CFR Part 164, 42 CFR Part 2, and other pertinent federal laws and regulations.

The Contractor shall establish and implement identity management, login and authentication procedures, including those that determine role-based access, and physical, network, and data security measures reasonably acceptable to the State to protect against unauthorized access to, or alteration, loss, destruction or commingling of, State Data and against unauthorized access to State systems, networks, and computers through the Contractor’s or its contractor’s servers or other facilities, software or services.

The Contractor represents and warrants that, during the term of this Contract, the Contractor shall use best effort to keep information systems free of any and all “time bombs,” viruses, copy protect mechanisms, backdoors, or other disclosed or undisclosed features which may (i) disable or damage State systems, networks, computers, devices, software, data, or any Portals or Web-Enabled Applications; (ii) render Web-Enabled Applications incapable of operation; (iii) permit access unauthorized by the State to any State system, network, computer, or website, or (iv) permit Portals or Web-Enabled Applications to be locked or disabled by the Contractor or any third party without the State’s consent. The Contractor further represents and warrants that, during the term of this Contract, the Contractor shall promptly correct, repair, or disable any “time bombs,” viruses, copy protect

mechanisms, backdoors, or other features described in the previous sentence promptly upon discovery at no cost to the State.
The Contractor shall cooperate with the State's reasonable requests for changes in security procedures.

The Contractor shall provide the State with 30 Days' prior written notice of any changes to security procedures and shall at all times provide the State with a current copy of its Information Security Plan.

7.4 **Information System End User Support**

Information System End User Support services shall include:

- Management of end user inquiries for the State, provider, and member users;
- Management of end user-reported problems;
- Management of end user support materials: printed reference materials for end users, online reference resources for end users; and
- If applicable, support for help desk vendor(s): knowledge bases for said vendors and troubleshooting support.

Deliverables:

a. Information System Operations, Maintenance and Support Services (OMSS) Plan – The Contractor shall develop a comprehensive Information System OMSS Plan, which shall be updated on an annual basis and approved by the State. At a minimum the OMSS Plan shall address:

- Ensuring the Contractor's information systems continually meets State requirements and is updated with new or revised functionality (i.e., via development and configuration) to support new requirements as a result of programmatic, operational, organizational, legal or regulatory changes that are agreed upon via the Change Management process;
- Accommodating changes to regulations, standards, and State organizational processes through operational and system changes that do not require significant system functional changes (i.e., development or configuration);
- Making improvements or changes in response to feedback collected from information system users via regular surveys and other forms of engagement such as focus groups/interviews;
- Ensuring interfaces are adequately supported and maintained to support all data exchange partners;
- Ensuring data in information systems is high quality, including a plan for correcting data containing errors;
- Ensuring that information system maintenance windows do not interfere with State business or occur during business hours;
- Providing regular and periodic maintenance to the solution on a schedule agreed upon by the Contractor and the State;
- Ensuring that solution knowledge transfer materials, manuals and reference guides, and technical documentation are kept up to date throughout the life of the contract; and
- Ensuring that all maintenance and support processes are articulated to the satisfaction of the State.

The OMSS plan shall incorporate the following elements:

- Scope;
- Resource Roles and Responsibilities;
- Configuration Management Protocol;
- Change Management Protocol internal to the Contractor;

- Operations and Hosting (O&H) Plan – The Contractor shall develop a comprehensive Solution Operations and Hosting plan, which will be updated on an annual basis and approved by the State. The O&H Plan must, at a minimum, incorporate the following elements:

    - Scope;
    - Resource Roles and Responsibilities;

- Job/Job Stream Processing Protocol;
- Availability and Performance Monitoring and Tuning Protocols;
- Availability and Performance Measures;
- Key Performance Indicators;
- Incident Reporting and Management Protocols; and
- As applicable, any plans to address deficiencies found in audits.

- Information System Availability Assurance and Disaster Recovery Plan **–** The Contractor shall develop and maintain an Information System Availability Assurance and Disaster Recovery Plan (AA-DR) Plan that articulates how the solution shall be maintained and returned to normal operating conditions in the event of any man-made or natural disaster.

  In order to create the AA-DR Plan, the Contractor shall perform an Information Technology inventory, impact analysis, and risk analysis to identify threats and vulnerabilities, and identify their potential impact on the solution.

  The AA-DR Plan shall include, at a minimum: continuity of operations and disaster recovery goals; information system inventory; assessment of availability and disaster recovery risks, vulnerabilities and business impact; roles and responsibilities; communication strategies; back up procedures; availability assurance provisions and procedures; disaster recovery provisions and procedures; and information system restoration procedures. The Contractor shall refer to and utilize best practices for disaster management, such as National Institute of Standards and Technology (NIST) contingency planning guidance.
- Information System Security Risk Management Plan **–** The Contractor shall provide an Information System Security and Risk Management Plan consistent with State application guidelines published by BIT and leverages industry standard guidelines such as the NIST cybersecurity framework. The purpose of the Plan is to ensure the Contractor appropriately mitigates and manages security risk, including what it will do to identify, protect against, detect, respond to, and recover from security risks. The Information System Security and Risk Management Plan shall include, at a minimum: roles and responsibilities; risk assessment, including ranking system for security risks accounting for risk probability, severity, and other criteria; risk treatment, including how the Contractor will remediate, mitigate, avoid, accept, transfer or otherwise manage the risks; and any other items deemed necessary by the State.

- Information Security Plan – The Contractor shall provide an Information Security Plan that meets all pertinent requirements published by BIT and leverages industry standard guidelines such as the NIST security framework. The Information Security Plan must include, at a minimum: roles and responsibilities; overview of any relevant laws or regulations; data protection risks; acceptable use policies; data utilization; data storage security requirements, including backed-up data; and data integrity and assurance including how to securely store and transfer data. The Information Security Plan must also incorporate the Contractor's Data Classification System, where it will outline the applicable levels of access associated with specific data elements maintained in its information systems.

b. Maintenance and Support Activity Reports – The Contractor shall produce reports that detail maintenance and support activity, including system and capacity monitoring and preventive approaches; these reports will enable the State to gauge maintenance and support activity and to identify trends in support activity that can lead to process improvement, training and other efforts aimed at reducing noted issues. The criteria governing the activity types which will be included in these reports will be agreed to between the Contractor and the State.

Incident Reports – Information System Operations – The Contractor shall produce reports that detail incidents associated with solution operations and hosting activity (e.g., a firmware update that had to be backed out and subsequently reapplied after further testing was conducted). The reports shall indicate the cause of any incidents and how the incident was resolved. The criteria governing the incident types which will be included in these reports will be agreed to between the Contractor and the State.

c. Incident Reports – Information System Maintenance – The Contractor shall produce reports that detail incidents associated with solution maintenance activity, e.g., a security patch that had to be backed out and subsequently reapplied after further testing was conducted. The reports shall indicate the cause of any incidents and how the incident was resolved. The criteria governing the incident types which will be included in these reports will be agreed to between the Contractor and the State.

d. Information System Availability and Performance Reports – The Contractor shall produce reports that detail availability and performance of the solution as a whole and, as deemed applicable, the availability and performance of select components. Availability and performance shall be measured according to the standards set forth in Attachment XXX.

8. Key Performance Indicators (KPIs)

To ensure that the solution information systems continuously meet availability and performance expectations throughout the life of the contract, the Contractor will be held accountable using a Key Performance Indicator (KPI) framework as described in Attachment XXX.
Each year's KPI targets will be agreed upon by the State and the Contractor following a review of the Contractor's performance in the prior year.

8.1 KPI Capture, Tracking and Evaluation

The Contractor and the State will work to establish an automated system to capture KPI statistics agreed upon by the Contractor and the State and support KPI tracking and evaluation according to the Annual KPI Plan. The Contractor shall report on KPIs as specified in this contract. the State reserves the right to conduct an audit of how KPI statistics are generated and provided.
If and as directed by the State, all KPI information shall be stored in tables, databases or other formats approved by the State Project Manager and accessible by designated the State personnel. Additionally, if and as directed by the State KPIs shall be tracked through dashboards, reports or other appropriate tools.

The Contractor shall maintain supporting documentation for any KPI calculations. The supporting documentation for any KPI shall be delivered to the State Project Manager within two (2) business days after it is requested.

Deliverables:

a. **Annual KPI Plan** – The Contractor will produce an Annual KPI Plan that includes how the Contractor intends to achieve, measure, and, if applicable, report on the KPIs set forth in Attachment XXX. Annual review of the Annual KPI Plan will allow the State and the Contractor to review the Contractor's performance and provide the State and the Contractor the opportunity to add, delete, or modify KPIs, as well as adjust the allocation of value across KPIs for the calculation of Credits and Additional Charges. The Annual Plan will be approved by the State Project Manager following any necessary discussions with the Contractor. The initial Annual KPI Plan will be completed as part of the Project Initiation phase. Subsequent plans will be completed annually and will include a plan for reporting (e.g., monthly, quarterly, annually) on the Contractor's performance on KPIs.

9. Turnover

The Contractor shall be responsible for all requirements listed in this RFP up to the date of termination of contract.

The Contractor shall develop and, if required, execute a turnover plan intended to provide for an orderly, controlled transition of the Contractor's responsibilities to a successor contractor at the conclusion or termination of the contract period. The turnover plan will be designed to minimize disruption of services provided to the State. The Turnover Plan will establish a turnover schedule for the Contractor to comply with the requirements set forth in this section and, where appropriate, coordinate with related and/or dependent activities with the successor contractor. Additionally, the Turnover Plan will establish the procedures the Contractor shall follow to complete turnover activities, including submission of any turnover deliverables to the State for review and approval.

Deliverables:

a. **Turnover Plan**

The Contractor shall deliver a turnover plan per the State-approved Implementation Plan, acceptable to the State in its sole discretion. The turnover plan and any modification or updates must be prior approved by the State. The turnover plan must be updated at least annually.
At a minimum, the Turnover Plan will include the following components:

- Tasks and procedures
- Schedule
- Staffing supporting turnover activities
- Knowledge transfer and training
- Delivery of project documentation, including technical design, business design, business standard operational procedures, testing, pending findings, defects, change requests and others.
- Delivery of operational documentation and work artifacts
- Unencumbered transfer of data and other assets, as applicable
- Certificate(s) of destruction; as applicable
- Project communication associated with risk management and project status reporting during the transition
- Closeout task and event checklist

10. Information System Usage Rights

During the term of this Contract, the Contractor shall grant the right to use the solution to designated, authorized users without any licensing restrictions and at no cost to external end users.

11. Information Ownership and Governance

Except as otherwise agreed in writing between the Contractor and the State, all information generated as a result of the Contractor's operations in support of this contract is deemed State Data. For the purposes of this Contract, "State Data" means any data or information supplied by the State or any User to or through the solution, and any reports, databases, data queries, responses to data queries, or other output generated by the solution using or based on such data or information.

The Contractor shall establish and implement archiving and regular backup procedures acceptable to the State to ensure that a backup file set that is not more than 24 hours old is always available, and that the State Data is not inadvertently or deliberately discarded without the State's express consent. Procedures shall include offsite storage rotation. The Contractor shall not archive or destroy data and information relating to the State except in accordance with those archiving and backup procedures and other applicable provisions of this Contract. The Contractor shall provide the State with 30 Days' prior notice of any proposed changes to its archiving and backup procedures and shall at all times provide the State with a current copy of said procedures.

ATTACHMENT G – KPI Appendix

This must be downloaded as the Excel document
RFP_2814_Attachment_G-KPI_appendix.xlsx

ATTACHMENT H – Security and Contrqactor Questions

This must be downloaded as the PDF document
RFP_2814_Attachment_H-Security_and_Vendor_Questions.pdf

NOTE: If you woud like a Word version of this please contact Dawson.Lewis@state.sd.us with the subject line ***RFP 2814 Security and Vendor Questions in WOrd***

Security and Vendor Questions

Agencies: The following questions facilitate agencies acquiring technology that meets state security standards. These questions will assist in improving the quality and the timeliness of the procurement. BIT recommends that you utilize your BIT Point of Contact to set up a planning meeting to review the project and these questions. Understanding the background and context of the questions greatly improves realizing the purpose of the questions. Again, the purpose of the questions is to ensure the product/service being procured will meet the technology and security standards.

If you do not know the details of the technologies that vendors will propose, it is best to keep the question set as broad as possible. If there is a detailed knowledge of what will be proposed, a narrowed set of questions may be possible. Vendors are invited to mark any question that does not apply to their technology as NA (Not Applicable).

Contractors: The following questions help the state determine the best way to assess and integrate your product or service technology with the state's technology infrastructure. Some questions may not apply to the technology you use. In such cases, simply mark the question as NA (Not Applicable). You will see that these questions are divided into sections to help identify the point of the questions.

Use the last column as needed to explain your answers. Also note that many questions require you to explain your response. The more detailed the response, the better we can understand your product or service.

Where we feel that a Yes/No/NA response is not appropriate, the cell has been greyed out. **If the contractor answers a question by referencing another document or another part of the RFP response, they must give the page number and paragraph where the information can be found.**

The "BIT" column corresponds to the branch that will be the primary reviewers. If you have questions about the meaning or intent of a question, we can contact them on your behalf. DC = Data Center; DEV = Development; TEL = Telecommunications; POC = Point of Contact

ATTACHMENT I – Cost Proposal Worksheet

This must be downloaded as the Excel document
RFP_2814_Attachment_I-Cost_Proposal_Worksheet.xlsx

ATTACHMENT J – Information Technology Security Policy (ITSP)

This must be downloaded as the PDF document
RFP_2814_Attachment_J_Information_Technology_Security_Policy-Contractor.pdf

ATTACHMENT K – SECURITY ACKNOWLEDGEMENT FORM

Security Acknowledgement

Please return agreement to your BIT Manager or Designated BIT Contact

All BIT employees and State contractors must sign; **Agreement to Comply with BIT Information Technology Security Policy (the "Policy").** Users are responsible for compliance to all information security policies and procedures. *By signature below, the employee or contractor hereby acknowledges and agrees to the following:*

1. Employee is a State of South Dakota employee or contractor that uses non-public State of South Dakota technology infrastructure or information;
2. Employee or contractor will protect technology assets of the State from unauthorized activities including disclosure, modification, deletion, and usage;
3. Employee or contractor agrees to follow state and federal regulations in regards to confidentiality and handling of data;
4. Employee or contractor has read and agrees to abide by the Policy;
5. Employee or contractor consents to discuss with a supervisor / State contact regarding Policy violations;
6. Employee or contractor shall abide by the policies described as a condition of continued employment / service;
7. Employee or contractor understands that any individual found to violate the Policy is subject to disciplinary action, including but not limited to, privilege revocation, employment termination or financial reimbursement to the State;
8. Access to the technology infrastructure of the State is a privilege which may be changed or revoked at the discretion of BIT management;
9. Access to the technology infrastructure of the State automatically terminates upon departure from the State of South Dakota employment or contract termination;
10. Employee or contractor shall promptly report violations of security policies to a BIT manager or State Contact and BIT Help Desk (605.773.4357);
11. The Policy may be amended from time to time. The State of South Dakota recommends employees and contractors for the State to regularly review the appropriate Policy and annual amendments.

Information Technology Security Policy – BIT: http://intranet.bit.sd.gov/policies/
Information Technology Security Policy – CLIENT: http://intranet.bit.sd.gov/policies/
Information Technology Security Policy – CONTRACTOR: http://bit.sd.gov/vendor/default.aspx

Acknowledgement: State of South Dakota Information Technology Security Policy

Contractor: If the individual is signing for their entire company by signing this form the individual affirms that they have the authority to commit their entire organization and all its employees to follow the terms of this agreement.

Employee or Contractor signature _____ Date _____ BIT Manager or Contact _____ Date _____

Employee or Contractor name and Company name in block capital letters _____